PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-252654**
(43)Date of publication of application : **06.09.2002**

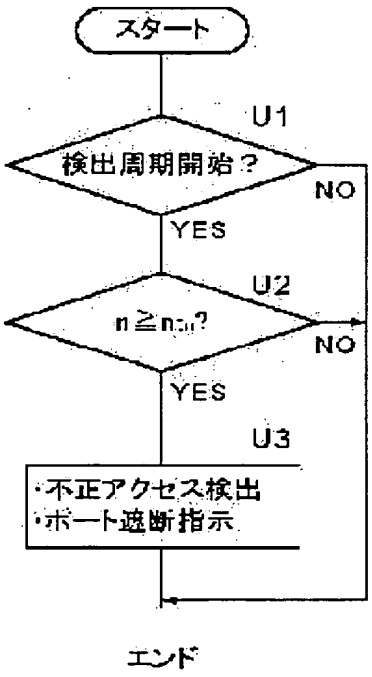
(51)Int.Cl. **H04L 12/66**
G06F 13/00

(21)Application number : **2001-048083**
(22)Date of filing : **23.02.2001**

(71)Applicant : **MITSUBISHI ELECTRIC CORP**
(72)Inventor : **KINOSHITA YOSUKE**

(54) INTRUSION DETECTION DEVICE, SYSTEM, AND ROUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an intrusion detection device capable of detecting an unauthorized access intrusion such as DDoS(distributed denial of service) attack automatically with high accuracy.
SOLUTION: An intrusion detection unit of a router acquires from a communication route a packet which reaches at the router, and generates a structure corresponding to each session based on network layer data and transport lay data described in the header of the packet. This structure is discarded when the session is terminated normally. The intrusion detection unit inspects the total number n of structures for each prescribed period. If there is any structure with a prescribed threshold nth or more as a result of the inspection, the unit detects it as the unauthorized access intrusion occurrence. Since a structure is generated for each session and the presence/absence of the unauthorized access intrusion is detected, based on the number of the generated structures, a DDoS attack, which establishes a large volume of different sessions, can be detected automatically with high accuracy.



LEGAL STATUS

[Date of request for examination] 21.10.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－252654
（P2002－252654A）
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ　５Ｂ０８９
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00	３５３Ｃ　５Ｋ０３０

審査請求　未請求　請求項の数11　ＯＬ　（全 22 頁）

(21)出願番号　特願2001－48083(P2001－48083)

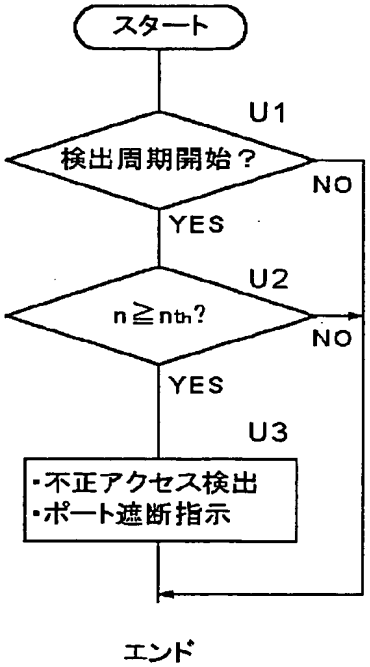
(22)出願日　平成13年２月23日(2001.2.23)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　木下　洋輔
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外１名）

Ｆターム(参考)　5B089 GA31 GB02 HB18 HB19 KA17
KB13 KC47 KG03 KG10 MC01
5K030 GA15 HA08 HC01 HD03 KA01
KA05 KA13

(54)【発明の名称】　侵入検出装置およびシステムならびにルータ

(57)【要約】
【課題】　ＤＤｏＳ攻撃などの不正アクセスの侵入を自動的にかつ高精度に検出できる侵入検出装置を提供する。
【解決手段】　ルータの侵入検出部は、ルータに到達するパケットを通信路から取得し、当該パケットのヘッダに記述されているネットワーク層（ＩＰ層）およびトランスポート層（ＴＣＰ層）のデータに基づいてセションごとに対応する構造体を生成する。この構造体は、セションが正常終了した場合に破棄される。侵入検出部は、所定の検査周期ごとに、構造体の総数ｎを検査する。その結果、所定の不正検出しきい値ｎth以上の構造体があれば、不正アクセスの侵入があると検出する。セションごとに構造体を生成してその数に基づいて不正アクセスの侵入の有無を検出するから、大量の異なるセションを確立するＤＤｏＳ攻撃を自動的にかつ精度良く検出できる。



1

【特許請求の範囲】

【請求項１】　コンピュータネットワーク上に確立されるセションを介して伝送されるパケットを取得し、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて上記セションごとに対応する構造体を生成し、当該構造体が異常な数となる場合に、不正アクセスの侵入を検出する侵入検出装置。

【請求項２】　コンピュータネットワーク上に確立されるセションを介して伝送されるパケットを取得するパケット取得手段と、

このパケット取得手段により取得されたパケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、上記セションごとに対応する構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上であるか否かを判別する判別手段と、

この判別手段により上記構造体の数が上記不正検出しきい値以上と判別された場合に、不正アクセスの侵入を検出する検出手段とを含む侵入検出装置。

【請求項３】　請求項２において、さらに、セションが正常終了した場合に、当該セションに対応する構造体を破棄する構造体破棄手段を含む侵入検出装置。

【請求項４】　請求項３において、構造体生成手段は、上記取得されたパケット自体を構造体の一部として構造体を生成するものであり、

上記構造体の一部であるパケットを結合するパケット結合手段と、

このパケット結合手段によるパケット結合の結果パケットを正常に結合できなかった時点において、当該構造体の保留を決定する保留決定手段とをさらに含み、

上記構造体破棄手段は、上記パケット結合手段によるパケット結合の結果パケットを正常に結合することができた場合に、当該セションに対応する構造体を破棄するものである侵入検出装置。

【請求項５】　請求項４において、パケット結合手段は、一連のパケットをすべて取得した後にパケットを結合する、または、パケットを取得するたびにパケットを結合するものである侵入検出装置。

【請求項６】　複数の侵入検出装置およびこれら複数の侵入検出装置に接続された上位管理装置を含む侵入検出システムにおいて、

上記複数の侵入検出装置は、それぞれ、

コンピュータネットワーク上に確立されるセションを介して伝送されるパケットを取得するパケット取得手段と、

このパケット取得手段により取得されたパケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、上記セションごとに対応する

2

構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上であるか否かを判別する判別手段と、

この判別手段により上記構造体の数が上記不正検出しきい値以上と判別された場合に、上記上位管理装置に対して不正アクセス検出信号を送信する信号送信手段と、

上位管理装置から送信されてきた判定信号に基づいて、不正アクセスの侵入の有無を検出する検出手段とを有するものであり、

上記上位管理装置は、上記複数の侵入検出装置のすべてから上記不正アクセス検出信号を受信したか否かを判別する受信判別手段と、

この受信判別手段によりすべての侵入検出装置から不正アクセス検出信号を受信したと判別された場合に不正アクセスの侵入があることを示し、上記受信判別手段によりすべての侵入検出装置から不正アクセス検出信号を受信していないと判別された場合に不正アクセスの侵入がないことを示す上記判定信号を少なくとも不正アクセス検出信号を送信してきた侵入検出装置に対して送信する判定信号送信手段とを有するものである侵入検出システム。

【請求項７】　複数の侵入検出装置を含む侵入検出システムにおいて、

上記複数の侵入検出装置は、それぞれ、

コンピュータネットワーク上に確立されるセションを介して伝送されるパケットを取得するパケット取得手段と、

このパケット取得手段により取得されたパケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、上記セションごとに対応する構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上であるかか否かを判別する判別手段と、

この判別手段により上記構造体の数が上記不正検出しきい値以上と判別された場合に、他の侵入検出装置に対してアクセス状況を確認するアクセス状況確認信号を送信するアクセス状況確認手段と、

他の侵入検出装置からアクセス状況確認信号を受信した場合に、上記構造体生成手段により生成される構造体の数を含む返信信号を上記他の侵入検出装置に返信する返信手段と、

他の侵入検出装置から返信されてきた返信信号に含まれている構造体の数に基づいて、不正アクセスの侵入の有無を検出する検出手段とを有するものである侵入検出システム。

【請求項８】　請求項７において、上記複数の侵入検出装置は、さらに、上記不正検出しきい値の補正値である補正しきい値を記憶する補正しきい値記憶手段と、他の

侵入検出装置からアクセス状況確認信号を受信した場合に、上記不正検出しきい値を上記補正しきい値記憶手段に記憶されている補正しきい値に補正するしきい値補正手段とをそれぞれ有するものである侵入検出システム。

【請求項９】　請求項２ないし５のいずれかにおいて、さらに、上記パケット取得手段により取得されたパケットのヘッダに記述されているトランスポート層のデータに基づいて、対象サービスに対応するパケットであるか否かを判別するサービス種別判別手段を含み、

上記構造体生成手段は、上記サービス種別判別手段により取得されたパケットが対象サービスに対応するパケットであると判別された場合にのみ、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、セションごとに対応する構造体を生成するものである侵入検出装置。

【請求項１０】　請求項９に記載された侵入検出装置とおとりサーバとを含む侵入検出システムにおいて、

上記侵入検出装置は、さらに、上記サービス種別判別手段により取得されたパケットが対象サービスに対応するパケットでないと判別された場合に、当該パケットをコピーし、当該コピーされたパケットを上記おとりサーバに転送する手段を有し、

上記おとりサーバは、上記パケットを受信した場合に、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて、セションごとに対応する構造体を生成する構造体生成手段と、

この構造体生成手段により生成された構造体の数が所定の不正検出しきい値以上になったか否かを判別する判別手段と、

この判別手段により上記不正検出しきい値以上になったと判別された場合に、不正アクセスの侵入を検出する検出手段とを含む不正アクセス検出手段とを有するものである侵入検出システム。

【請求項１１】　パケットを中継するルータにおいて、請求項１ないし５のいずれかまたは請求項９の侵入検出装置と、

この侵入検出装置により不正アクセスの侵入が検出された場合に、パケット中継を自動的に禁止する手段とを含むルータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、分散サービス不能攻撃（DDoS attack. DDoS：Distributed - denial of service）および分散ポートスキャン攻撃などの不正アクセスの侵入を検出する侵入検出装置およびシステム、ならびに上記侵入検出装置が用いられたルータに関する。

【０００２】

【従来の技術】従来から、ＤｏＳ攻撃などの不正アクセスの侵入を検出する侵入検出装置（ＩＤＳ：Intrusion Detection System）が知られている。ＤｏＳ攻撃は、侵入者のコンピュータから攻撃対象のコンピュータに大量のパケットを短時間で送信し、攻撃対象のコンピュータのシステムリソースを費やさせることにより、当該コンピュータをダウンさせる行為のことである。

【０００３】上記の侵入検出装置は、そのような攻撃からコンピュータを保護すべく、たとえばルータに備えられ、通信路上を流れ当該ルータに到達する直前のパケットを取得し、当該パケットのヘッダに記述されている送信先ポートまたは送信元ポートに基づいてアクセス量を監視することにより、不正アクセスの侵入を検出している。より具体的には、パケットには、送信先ポートおよび送信元ポートを記述したヘッダが含まれている。侵入検出装置は、当該パケットヘッドから送信先ポートおよび送信元ポートを抽出し、たとえば１つの送信元から１つの送信先へのパケット量が異常に多い場合などに、不正アクセスであると検出する。なお、このような侵入検出装置は、一般にネットワーク型ＩＤＳと呼ばれている。

【０００４】

【発明が解決しようとする課題】ところで、最近では、複数の送信元から攻撃対象の送信先へ一斉にパケットを送信するＤＤｏＳ攻撃と言われるものがある。より具体的には、ＤＤｏＳ攻撃は、侵入者のコンピュータから第３者のコンピュータに対してエージェントと呼ばれるソフトウエアを通信網を介してインストールし、そのエージェントをリモート操作することにより攻撃対象のコンピュータに多くのパケットを送信させ、攻撃対象のコンピュータのシステムリソースを費やさせることにより当該コンピュータをダウンさせる行為のことである。

【０００５】このＤＤｏＳ攻撃においては、第３者のコンピュータが送信元となるため、到着するパケットのヘッダに含まれる送信元ポートは、異なる複数のものとなる。したがって、侵入検出装置は、大量のパケットが到着しても、単なるアクセス量の増加であると判断する可能性がある。そのため、従来の侵入検出装置では、ＤＤｏＳ攻撃などの不正アクセスを良好に検出することができないとの問題があった。なお、不正アクセスであるか否かは、コンピュータがダウンした後に管理者が手作業でログ解析などを行ってはじめて判明するものであり、システムダウンと合わせて非常に非効率的な作業をしなければならなかった。

【０００６】そこで、本発明の目的は、ＤＤｏＳ攻撃などの不正アクセスの侵入を自動的にかつ高精度に検出できる侵入検出装置およびシステムを提供することである。

【０００７】また、本発明の他の目的は、上記侵入検出装置を用いることにより、不正アクセス侵入による被害拡大を迅速に防止できるルータを提供することである。

【０００８】

5

【課題を解決するための手段】上記目的を達成するためのこの発明は、コンピュータネットワーク上に確立されるセションを介して伝送されるパケットを取得し、当該パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいて上記セションごとに対応する構造体を生成し、当該構造体が異常な数となる場合に、不正アクセスの侵入を検出するものである。

【０００９】

【発明の実施の形態】以下では、本発明の実施の形態を、添付図面を参照して詳細に説明する。

【００１０】実施の形態１

図１は、本発明の実施の形態１に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。このコンピュータネットワークは、インターネットなどの外部ネットワーク１と、当該外部ネットワーク１に対してパケットを中継するルータ２を介して接続され、企業などの組織内に構築された内部ネットワーク３とを有するものである。

【００１１】外部ネットワーク１には、複数のコンピュータ４が接続されている。この外部ネットワーク１のコンピュータ４は、代表的には、パーソナルコンピュータおよびワークステーションである。内部ネットワーク３には、複数のコンピュータ５が接続されている。この内部ネットワーク３のコンピュータ５は、代表的には、パーソナルコンピュータ、メールサーバ、ウェブサーバおよびＦＴＰ(File Transfer Protcol)サーバである。

【００１２】外部および内部ネットワーク１、３の各コンピュータ４、５は、ＴＣＰ／ＩＰ(Transmission Control Protcol / Internet Protcol)を通信プロトコルとして使用し、パケットを送受信する機能を有している。ここに、ＴＣＰは、ＯＳＩ(Open Systems Interconnection)参照モデルにおけるトランスポート層の通信プロトコルであり、ＩＰは、ＯＳＩ参照モデルにおけるネットワーク層の通信プロトコルである。なお、通信プロトコルは、ＴＣＰ／ＩＰに限定されるものでなく、ＡＲＰ(Address Resolution Protocol)、ＲＡＲＰ(Reverse Address ResolutionProtocol)、ＩＰＸ(Internetwork Packet Protocol)、ＮｅｔＢＩＯＳ(NetworkBasic Input Output System)、ＩＣＭＰ(Internet Control Message Protocol)、ＩＧＭＰ(Internet Group Management Protocol)、ＳＰＸ(Sequenced PacketExchange)、ＮＣＰ(Network Control Protocol)、ＲＩＰ(Routing InformationProtocol)、ＮＬＳＰ(Netware Link Service Protocol)、ＳＡＰ(Service Advertising Protocol)などの他の通信プロトコルでもよいことはもちろんである。

【００１３】各コンピュータ４、５は、正常なパケット通信を実行する場合、トランスポート層の通信プロトコルであるＴＣＰに従って相手方コンピュータとの間でセションを確立し、信頼性のあるパケット通信を実現する。より具体的には、発呼側および着呼側のコンピュータ間でいわゆる３ウェイハンドシェイクが実行されることによりセション（論理的通信路）が確立される。

【００１４】さらに具体的には、発呼側のコンピュータは、回線接続要求パケットを着呼側のコンピュータに対して送信する。着呼側のコンピュータは、当該回線接続要求に対して接続応答パケットを返信する。この際、着呼側のコンピュータは、これから確立しようとしているセションを識別する情報としてセション識別子を発呼側のコンピュータに割り当てる。

【００１５】これに応答して、発呼側のコンピュータは、パスワード等の通信に必要なデータを含むパケットを着呼側のコンピュータに返信する。このとき、発呼側のコンピュータは、上記着呼側のコンピュータから割り当てられたセション識別子を上記パケットのヘッダに記述する。着呼側のコンピュータは、上記通信に必要なデータを受け取ると、発呼側のコンピュータに対して通信許可パケットを通知する。こうして、セションが確立する。

【００１６】以後、発呼側のコンピュータからパケットを送信する際には、上記割り当てられたセション識別子をヘッダに記述する。すなわち、セションを正常に確立しようとしそれが実際に確立されれば、着呼側のコンピュータには、発呼側のコンピュータから同一のセション識別子を有する複数のパケットが送信されてくることになる。

【００１７】一方、不正アクセス時には、発呼側のコンピュータにインストールされているエージェントと呼ばれる不正ツールは、通常、着呼側のコンピュータとの間で正常なセションを確立しようとすることなく、一方的にパケットを着呼側のコンピュータに対して送信し続ける。この場合、パケットのヘッダには、通常、適当なセション識別子が記述される。したがって、不正アクセス時には、複数の異なるセション識別子をそれぞれ有する複数のパケットが不正アクセス元のコンピュータから着呼側のコンピュータに送信されることになる。

【００１８】なお、上述のように、不正アクセス時には正常な意味でのセションは確立されていないけれども、本実施の形態１においては、パケットを着呼側のコンピュータに送り込む論理的な通信路が形成されているという意味において、セションが確立されているとみなすこととしている。

【００１９】本実施の形態１に係るルータ２は、不正アクセス時には複数の異なるセション識別子をそれぞれ有するパケットが送信されてくることに着目し、セション識別子ごとに、すなわちセションごとに、そのセションに関する情報を記述する構造体を生成し、当該構造体が異常な数になった場合に、不正アクセスの侵入を検出している。より具体的には、ルータ２は、コンピュータネットワーク上に確立されたセションを介して伝送されて

6

いるパケットを取得する。言い替えれば、ルータ２は、通信路上を流れているパケットを取得する。その後、ルータ２は、各セションに対応する構造体を生成して保持し、当該構造体の総数が所定の不正検出しきい値ｎth以上になった場合に、不正アクセスの侵入を検出する。ここに、構造体を構成するセションに関する情報とは、送信元ＩＰアドレス、送信先ＩＰアドレス、送信元ポートおよび送信先ポートなどのセション基本情報、ならびに最終パケット到着時刻および総パケット数などのセション拡張情報である。

【００２０】ただし、アクセス量の増加に伴って正常なセションが大量に確立される場合もあり、この場合上記構造体もそのセションの数に応じて生成されることになるから、上述の判断基準のみでは、正常なアクセスを不正アクセスと誤検出するおそれがある。

【００２１】そこで、本実施の形態１に係るルータ２は、正常なセションに対応する構造体については所定の破棄条件を満足したことに応答して破棄することとしている。上記所定の破棄条件は、正常なセションに対してのみ該当する条件である。たとえば、上記所定の破棄条件は、セションが正常に終了したことである。セションが正常に終了したか否かは、たとえば、セション開始時刻、最終パケット到着時刻および総パケット数などのセション拡張情報を参照し、比較的短時間で一連のパケットをすべて受信したか否かにより判断できる。したがって、残っていく構造体のほとんどは、不正アクセスに対応するものとなる。そのため、構造体の数を見るだけでも、正常なアクセスを不正アクセスと誤検出することを防止できる。

【００２２】しかも、セションが正常に確立しているか否かを反映する構造体を参照して不正アクセスの検出を行っているから、従来のように送信先ポートおよび送信元ポートを監視するだけでは困難であったＤＤｏＳ攻撃を自動的にかつ高精度に検出することができる。

【００２３】図２は、パケットの構成を示す概念図である。パケットは、ヘッダおよびデータを含む。ヘッダは、たとえば、ネットワーク層およびトランスポート層など複数の通信プロトコル層のデータを有している。具体的には、ヘッダには、送信元ＩＰアドレス、送信先ＩＰアドレス、パケット長および１つのセションに固有のセション識別子がネットワーク層のデータとして記述されている。また、ヘッダには、送信元ポート、送信先ポート、パケットの送信順序を表しているシーケンス番号がネットワーク層のデータとして記述されている。

【００２４】さらに、ヘッダには、たとえば、次パケットのパケット長が図２におけるビットフラグおよびフラグメントオフセットに記述されている。また、最後のシーケンス番号に対応するパケットのヘッダには、たとえば、最後のパケットであることを示す最終パケットデータが図２におけるビットフラグに記述されている。さらに、ヘッダには、当該一連のパケットの総数が図２におけるビットフラグに記述されている。

【００２５】図３は、ルータ２の内部構成を示すブロック図である。ルータ２は、上述のように、外部ネットワーク１からのアクセスを監視し、不正アクセスの侵入を検出した場合、以後の内部ネットワーク３への侵入を拒絶する機能を有している。より具体的には、ルータ２は、ルーチング部１０および侵入検出部１１を備えている。

【００２６】ルーチング部１０は、外部ネットワーク１から通信路１２上を流れルータ２に到達するパケットを内部ネットワーク３に中継したり、内部ネットワーク３から出力されるパケットを外部ネットワーク１に中継したりする。この場合、ルーチング部１０は、侵入検出部１１の検出結果を参照して中継処理を実行する。

【００２７】侵入検出部１１は、ルータ２に到達するパケットのヘッダを監視することにより不正アクセスの侵入を検出する。より具体的には、侵入検出部１１は、しきい値記憶部１１ａおよび構造体記憶部１１ｂを有している。しきい値記憶部１１ａは、上記不正検出しきい値ｎthを記憶するものである。不正検出しきい値ｎthは、当該ルータの管理者が任意に設定できるものであり、たとえば、これ以上の数であればアクセス量の増加が異常であると考えられる値に設定される。構造体記憶部１１ｂは、上記構造体を記憶するものである。

【００２８】侵入検出部１１は、ルータ２に到達するすべてのパケットを取得し、当該パケットのヘッダを抽出し、セションを識別する。侵入検出部１１は、この識別されたセションに従って構造体を生成し、上記構造体記憶部１１ｂに記憶させる。侵入検出部１１は、この構造体記憶部１１ｂに記憶されている構造体の総数ｎが上記しきい値記憶部１１ａに記憶されている不正検出しきい値ｎth以上であるか否かに基づいて、不正アクセスの侵入の有無を検出する。もしも不正アクセスの侵入を検出した場合、侵入検出部１１は、ルーチング部１０にアクセスし、外部ネットワーク１に繋がっている接続ポートを封鎖する。こうして、不正アクセスの被害から内部ネットワーク３を保護している。

【００２９】侵入検出部１１は、たとえば、ルータ２に実装されるコンピュータボードである。より具体的には、当該コンピュータボードは、コンピュータプログラムを記憶しているＩＣ(Integrated Circuit)およびメモリを搭載するものであり、上記コンピュータプログラムの１つは、不正アクセス検出プログラムである。すなわち、より詳細に見れば、侵入検出部１１は、上記不正アクセス検出プログラムを記憶しているＩＣおよびメモリである。

【００３０】図４は、構造体を示す概念図である。上述のように、構造体は、セションごとに生成されるものである。構造体は、各セションごとに、セション基本情報

およびセション拡張情報を含む。セション基本情報は、送信元ＩＰアドレスおよび送信先ＩＰアドレス、セション識別子などのネットワーク層の情報と、送信元ポートおよび送信先ポートなどのトランスポート層のデータと、論理的に隣接する構造体のアドレスを記述するセション情報ディスクリプタポインタと、対応するセション拡張情報のアドレスを記述する次ディスクリプタとを有する。セション拡張情報は、ＩＰセション開始時刻と、ＴＣＰセション開始時刻と、最終パケット到着時刻と、侵入検出部１１により取得されたパケットの総数である総パケット数とを有する。なお、連鎖構造の最後の構造体における次ディスクリプタポインタには、ヌル（ＮＵＬＬ）値が記述される。

【００３１】図５、図６および図７は、侵入検出部１１において実行される不正アクセス検出処理を説明するためのフローチャートである。不正アクセス検出処理は、複数の処理から構成されている。具体的には、不正アクセス検出処理は、構造体生成／破棄処理、構造体破棄処理および構造体数検査処理からなる。

【００３２】図５は、構造体生成／破棄処理を説明するためのフローチャートである。侵入検出部１１は、ルータ２に到達するパケットを通信路１２から取得し（ステップＳ１）、当該パケットからヘッダを抽出する（ステップＳ２）。その後、侵入検出部１１は、当該ヘッダ中のセション識別子に基づいて、構造体を生成する（ステップＳ３～Ｓ５）。

【００３３】より具体的には、侵入検出部１１は、参照されたセション識別子と同じセション識別子の構造体が構造体記憶部１１ｂに記憶されているか否かを検索する（ステップＳ３）。同じセション識別子の構造体があれば（ステップＳ３のＹＥＳ）、侵入検出部１１は、当該構造体を更新する（ステップＳ４）。より具体的には、侵入検出部１１は、最終パケット到着時刻および総パケット数を更新する。一方、同じセション識別子の構造体がなければ（ステップＳ３のＮＯ）、侵入検出部１１は、当該セション識別子に対応する構造体を新たに生成する（ステップＳ５）。すなわち、侵入検出部１１は、図４に示されたような構造体を生成し、当該構造体を構造体記憶部１１ｂに記憶させる。

【００３４】また、侵入検出部１１は、取得されたパケットのヘッダに最終パケットであることが記述されているか否かを判別する（ステップＳ６）。最終パケットでなければ（ステップＳ６のＮＯ）、侵入検出部１１は、当該処理を終了する。一方、最終パケットであれば（ステップＳ６のＹＥＳ）、侵入検出部１１は、当該最終パケットのヘッダに記述されている総パケット数と構造体に記述している総パケット数とを比較し、一致しているか否かを判別する（ステップＳ７）。一致していなければ（ステップＳ７のＮＯ）、途中のシーケンス番号に対応するパケットの到着が遅れている可能性があるため、侵入検出部１１は、構造体の破棄を一時的に保留する（ステップＳ８）。一方、一致していれば（ステップＳ７のＹＥＳ）、一連のパケットをすべて受信しセションが正常に終了したものと考えられるから、侵入検出部１１は、当該セションに対応する構造体を破棄する（ステップＳ９）。

【００３５】上述のように、侵入検出部１１は、一連のパケットをすべて受信した場合にセションが正常に終了したものとして、当該セションに対応する構造体を破棄する。しかし、最終パケットの受信を確認したのに途中のパケットが遅れているためだけに構造体を一時保留し破棄できない場合がある。そこで、侵入検出部１１は、このような構造体を確実に破棄すべく、上記構造体生成／破棄処理と並列に、図６に示された構造体破棄処理を実行する。

【００３６】構造体破棄処理を実行する場合、侵入検出部１１は、一定周期ごとに、構造体をスキャンする。より具体的には、侵入検出部１１は、一定周期が開始されたことに応答して（ステップＴ１のＹＥＳ）、１つ目の構造体を対象とし（ステップＴ２）、当該構造体中のセション拡張情報の１つである最終パケット到着時刻を参照し、最終パケットが到着してから一定時間以上経過しているか否かを判別する（ステップＴ３）。さらに具体的には、侵入検出部１１は、最終パケット到着時刻と現在時刻とを比較し、上記一定時間以上経過しているか否かを判別する。上記一定時間は、管理者が任意に設定可能なもので、たとえば１日、３日、１週間などである。

【００３７】上記一定時間以上経過していれば、たとえば、発呼側のコンピュータで不具合が発生した、あるいは経由サーバで不具合が発生した、などが考えられる。しかも、不正アクセスでシステムダウンするのは短時間に大量のパケットが到着することを鑑みれば、最終パケット到着から時間が経過しているようなアクセスを不正アクセスとして検出する必要性はないと考えられる。そのため、上記一定時間以上経過していれば（ステップＴ３のＹＥＳ）、侵入検出部１１は、当該セションに対応する構造体を破棄する（ステップＴ４）。

【００３８】一方、一定時間以上経過していなければ（ステップＴ３のＮＯ）、パケットの送信途中であると考えられるから、侵入検出部１１は、すべての構造体についてのスキャンが終了したか否かを判別する（ステップＴ５）。すべての構造体についてのスキャンが終了していなければ（ステップＴ５のＮＯ）、侵入検出部１１は、次の構造体を対象とし（ステップＴ６）、上記ステップＴ３の処理に移行する。一方、すべての構造体についてのスキャンが終了していれば（ステップＴ５のＹＥＳ）、侵入検出部１１は、当該処理を終了する。

【００３９】以上の処理により、侵入検出部１１は、正常なセションに対応する構造体については随時破棄していくことになる。したがって、残っていくのは、不正ア

クセスに対応する構造体ということになる。一方、ＤＤｏＳ攻撃のような不正アクセスは、上述のように、大量の不正なセションを通して大量のパケットを送信し続けるから、残っている構造体の数が多ければ、不正アクセスであることを検出することができる。そこで、侵入検出部１１は、上記構造体生成／破棄処理および構造体破棄処理と並列に、図７に示された構造体数検査処理を実行する。

【００４０】侵入検出部１１は、保有している構造体の数を一定の検出周期Δｔごとに検査する。より具体的には、侵入検出部１１は、上記検査周期Δｔの開始に応答して（ステップＵ１のＹＥＳ）、保有している構造体の総数ｎが不正検出しきい値ｎth以上であるか否かを判別する（ステップＵ２）。構造体の総数ｎが上記不正検出しきい値ｎth未満であれば（ステップＵ２のＮＯ）、不正アクセスの侵入はないと考えられるから、侵入検出部１１は、当該処理を終了する。一方、構造体の総数ｎが不正検出しきい値ｎth以上であれば（ステップＵ２のＹＥＳ）、ＤＤｏＳ攻撃を含む不正アクセスの侵入があると考えられるから、侵入検出部１１は、ルーチング部１０にアクセスし、外部ネットワーク１との接続ポートを遮断させる（ステップＵ３）。

【００４１】以上のようにこの実施の形態１によれば、パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいてセションごとに対応する構造体を生成し、当該構造体の数が異常になれば、不正アクセスであると検出している。したがって、第３者のコンピュータにエージェントをインストールし単なるアクセス量の増加であると誤認させようとＤＤｏＳ攻撃を仕掛けても、当該ＤＤｏＳ攻撃を自動的にかつ高精度に検出することができる。そのため、従来よりもセキュリティ信頼度が向上されたシステム構築を実現することができる。

【００４２】また、正常アクセスに対応する構造体を確実に破棄しているから、構造体の総数に占めるＤＤｏＳ攻撃などの不正アクセスに対応する構造体の比率を高くすることができる。したがって、単なるアクセス量増加を不正アクセスであると誤検出する頻度を大幅に低減できる。そのため、不正アクセスを一層高精度に検出することができる。

【００４３】実施の形態２

上記実施の形態１では、セションが正常に終了したか否かに基づいて、構造体を保留するか否かを判別している。これに対して、本実施の形態２では、セションが正常に終了したか否かだけでなく一連のパケットを正常に結合できるか否かに基づいて、構造体を保留するか否かを判別することとしている。

【００４４】セションが正常に終了したか否かは、比較的短時間で一連のパケットをすべて受信したか否かに基づいて判断される。すなわち、最終パケットのヘッダに記述されている最終パケットデータおよび総パケット数に基づいて判断される。しかし、ヘッダの書き換えは相対的に容易に行えるため、厳密に言えば、不正アクセスであってもセションが正常に終了する場合がある。したがって、不正アクセスであるにもかかわらず、正常アクセスであると誤検出するおそれがある。一方、パケット長を変えたりすることは相対的に困難であるため、不正アクセスであればパケットを正常に結合することはできない。そこで、本実施の形態２では、パケットを正常に結合できるか否かに基づいて、構造体を保留するか否かを判別することとしている。

【００４５】さらに具体的には、正常な通信ツールから送信された複数のパケットであれば、侵入検出部１１において正常に結合することができる。より具体的には、正常なツールは、ＲＦＣに従って一連のデータを単純に複数のパケットに分割するだけなので、あるパケットのヘッダに記述されている次パケットに関するデータと実際に受信されるパケットとの間には整合性がある。たとえば、次パケットは数バイトのパケット長を有するとのデータがヘッダに記述されている場合、シーケンス番号から見た次パケットは確かにヘッダに記述されているのと同じパケット長を有している。したがって、侵入検出部１１は、パケットを正常に結合することができる。

【００４６】一方、不正ツールは攻撃対象のコンピュータにパケットを送り込むためのものであり上記ＲＦＣに従ってパケット生成を行っていないので、各パケットのヘッダに記述されている次パケットに関するデータと実際に受信されるパケットとの間には、通常、整合性はない。したがって、たとえば次パケットはｋバイトのパケット長を有するとのデータがヘッダに記述されている場合、シーケンス番号では次パケットでも上記ｋバイトとは異なるｉバイトのパケット長を有していることがある。そのため、パケットを正常に結合することができなくなる。

【００４７】図８は、本実施の形態２に係る構造体を示す概念図である。この構造体は、セション基本情報およびセション拡張情報に加えて、パケット自体を到着パケット情報をその一部とする。到着パケット情報は、ヘッダおよびデータの両方を含むパケット自体と、当該パケットの到着時刻と、直後に取得された到着パケット情報の先頭アドレスを指示する次パケットディスクリプタポインタとを含む。セション拡張情報は、到着パケット情報の先頭アドレスを指示する未生成パケット格納ディスクリプタポインタを有している。

【００４８】図９は、本実施の形態２に係る構造体生成／破棄処理である。すなわち、本実施の形態２では、上記実施の形態１のように構造体生成／破棄処理（図５）および構造体破棄処理（図６）を並列に行うのでなく、１つの構造体生成／破棄処理として実行するものである。なお、本実施の形態２においても、構造体数検査処

理は、当該構造体生成／破棄処理と並列に行われる。

【００４９】侵入検出部１１は、通信路１２からパケットを取得すると（ステップＶ１）、当該パケットのヘッダを抽出し（ステップＶ２）、当該ヘッダ中のセション識別子に基づいて構造体生成処理を実行する（ステップＶ３～Ｖ５）。

【００５０】より具体的には、侵入検出部１１は、当該セション識別子に対応する構造体が存在するか否かを判別する（ステップＶ３）。当該セション識別子に対応する構造体が存在していれば（ステップＶ３のＹＥＳ）、侵入検出部１１は、セション拡張情報の最終パケット到着時刻および総パケット数を更新するとともに、取得されたパケット自体を含む到着パケット情報を新たに生成し、当該到着パケット情報を構造体に追加する（ステップＶ４）。

【００５１】一方、上記セション識別子に対応する構造体が存在していなければ（ステップＶ３のＮＯ）、侵入検出部１１は、当該セション識別子に対応する構造体を新たに生成する（ステップＶ５）。この場合、侵入検出部１１は、セション基本情報、セション拡張および到着パケット情報を構造体として生成する。

【００５２】さらに、侵入検出部１１は、取得されたパケットのヘッダを参照し、当該パケットが最終パケットであるか否かを判別する（ステップＶ６）。最終パケットでなければ（ステップＶ６のＮＯ）、侵入検出部１１は、次に、既に取得され到着パケット情報として保持されているパケットの中に最終パケットがあるか否かを判別する（ステップＶ７）。パケットの送信経路によっては最終パケットが途中のパケットよりも先に到着することがあるからである。

【００５３】到着パケット情報の中にも最終パケットがなければ（ステップＶ７のＮＯ）、侵入検出部１１は、当該処理を終了する。一方、到着パケット情報の中に最終パケットがあれば（ステップＶ７のＹＥＳ）、侵入検出部１１は、一連のパケットをすべて取得したか否かを判別する（ステップＶ８）。また、ステップＶ６の結果、取得されたパケットが最終パケットであると判別された場合にも、当該ステップＶ８に係る一連のパケットをすべて取得したか否かの判別処理を実行する。

【００５４】当該判別処理は、取得された最終パケットまたは到着パケット情報として保持されている最終パケットのヘッダに記述されている総パケット数とセション拡張情報中の総パケット数とを比較し、一致しているか否かを判別する処理である。一致していなければ（ステップＶ８のＮＯ）、途中のパケットの到着が遅れていると考えられるから、侵入検出部１１は、当該処理を終了する。一致していれば（ステップＶ８のＹＥＳ）、一連のパケットがすべて取得されたと考えられるから、侵入検出部１１は、パケット結合処理を実行する（ステップＶ９～Ｖ１３）。すなわち、一連のパケットをすべて取得した後からパケット結合処理を実行する。

【００５５】より具体的には、侵入検出部１１は、各到着パケット情報のヘッダ中のシーケンス番号を参照し、先頭のシーケンス番号に係るパケットから順次累積的に結合していく。さらに具体的には、侵入検出部１１は、対象パケットと次パケットとを正常に結合できるか否かを判別する（ステップＶ９）。さらに具体的には、侵入検出部１１は、最初に先頭パケットを対象とし、当該先頭パケットのヘッダ中の次パケットのパケット長とシーケンス番号から見た場合における２番目のパケットのパケット長とが一致するか否かを判別する。一致していれば（ステップＶ９のＹＥＳ）、侵入検出部１１は、２番目のパケットを先頭パケットに結合する（ステップＶ１０）。

【００５６】その後、侵入検出部１１は、すべてのパケットの結合が終了したか否かを判別する（ステップＶ１１）。この場合、すべてのパケットの結合が終了していないので、侵入検出部１１は、２番目のパケットを対象とし、上記ステップＶ９の判別処理に移行する。パケットを正常に結合することができ、その結果すべてのパケットの結合が終了すれば（ステップＶ１１のＹＥＳ）、当該セションは正常セションであると考えられ、かつ正常アクセスであると考えられるから、侵入検出部１１は、当該構造体を破棄する（ステップＶ１２）。

【００５７】一方、ステップＶ９の結果、次パケット長と次パケットの実際のパケット長とが一致していなければ、不正パケットである可能性が極めて高いため、侵入検出部１１は、この時点で以後のパケットの結合処理を中止し、当該構造体の保留を決定する（ステップＶ１３）。

【００５８】図１０は、ルータ２の構成を機能的に説明するための概念図である。ルータ２は、通信プロトコルの階層として、物理層、データリンク（Ｄ／Ｌ）層、ＩＰ層、ＴＣＰ層および上位ＡＰ層を有している。また、ルータ２は、ネットワーク層であるＩＰ層およびトランスポート層であるＴＣＰ層の間にＩＤＳ層を有している。ルータ２に到達するパケットは、ＩＰ層およびＴＣＰ層を介してＩＤＳ層において処理され、ヘッダからデータまでを関連付けて監視される。すなわち、ネットワーク層よりも上位層でパケットが管理される。

【００５９】以上のようにこの実施の形態２によれば、一連のパケットを正常に組み立てることができるか否かに基づいて構造体を保留するか否かを決定している。したがって、不正パケットのセション識別子はパケットごとに異なるために本来ならば構造体が急激に増加するはずであるのに、セション識別子が不正に書き換えられて１つのデータ構造体しか生成されないような場合でも、その構造体が不正アクセスに対応しているものであることを検出できる。そのため、不正アクセスの侵入を精度良く検出できるので、ＤＤｏＳ攻撃などを精度良くかつ

自動的に検出できる。よって、セキュリティ信頼性のあるシステム構築を実現することができる。

【００６０】実施の形態３

上記実施の形態２では、一連のパケットをすべて取得した後にパケット結合処理を実行している。これに対して、本実施の形態３では、一連のパケットを取得している途中においてパケット結合処理を実行している。これにより、構造体の保留／破棄を迅速に決定でき、その結果ＤＤｏＳ攻撃などを迅速に検出することができる。

【００６１】上述のように、不正パケットにおいてはヘッダと実際のパケットとの間の整合性はないので、一連のパケットを取得している最中においても結合処理を行えば不正パケットであるか否かを判断することができる。そこで、本実施の形態３では、パケットが取得されるたびにパケットの結合処理を実行し、正常に結合できなかった時点においてその構造体を保留すると決定するようにしている。

【００６２】図１１は、本実施の形態３に係る構造体生成／破棄処理を説明するためのフローチャートである。本実施の形態３においても、上記実施の形態２と同様に、構造体生成／破棄処理および構造体破棄処理を１つの処理として実行し、かつ、当該構造体生成／破棄処理と並列に、構造体数検査処理を実行する。

【００６３】侵入検出部１１は、通信路１２からパケットを取得すると（ステップＷ１）、上述と同様に、当該パケットからヘッダを抽出し（ステップＷ２）、当該ヘッダ中のセション識別子に対応する構造体が存在するか否かを判別する（ステップＷ３）。構造体があれば（ステップＷ３のＹＥＳ）、侵入検出部１１は、当該構造体を更新する（ステップＷ４）。一方、構造体がなければ（ステップＷ３のＮＯ）、侵入検出部１１は、上記セション識別子に対応する構造体を新たに生成する（ステップＷ５）。

【００６４】また、侵入検出部１１は、既存の構造体を更新する際に、新たに取得されたパケットと取得済のパケットとの結合を試みる。より具体的には、侵入検出部１１は、取得されたパケットおよび既に保持されているパケットのヘッダに記述されているシーケンス番号に基づいて、取得されたパケットの前パケットまたは次パケットを検索し、いずれかに連続するパケットが保持されているか否かを判別する（ステップＷ６）。さらに具体的には、侵入検出部１１は、取得されたパケットのヘッダに記述されているシーケンス番号と保持されている１または複数のパケットのヘッダに記述されているシーケンス番号とを比較することにより、前パケットまたは次パケットを検索する。

【００６５】その結果、シーケンス番号から見て連続するパケットが保持されている場合（ステップＷ６のＹＥＳ）、侵入検出部１１は、取得されたパケットと当該連続するパケットとを結合できるか否かを判別する（ステップＷ７）。より具体的には、取得されたパケットの次パケットが保持されている場合、侵入検出部１１は、保持されている次パケットのパケット長が取得されたパケットのヘッダに記述されている次パケット長と一致するか否かを判別する。また、取得されたパケットの前パケットが保持されている場合、侵入検出部１１は、取得されたパケットのパケット長が保持されている前パケットのヘッダに記述されている次パケット長と一致するか否かを判別する。すなわち、連続するパケット間で整合性がとれているか否かに基づいて、結合可能であるか否かを判別することとしている。

【００６６】ヘッダに記述されている情報と整合性がとれていて結合可能である場合（ステップＷ７のＹＥＳ）、侵入検出部１１は、取得されたパケットと保持されているパケットとを結合する（ステップＷ８）。一方、シーケンス番号では確かに連続するパケットであるけれども次パケット長などのヘッダの情報から整合性がなく結合不能である場合（ステップＷ７のＮＯ）、侵入検出部１１は、この時点において当該構造体を保留することを決定する（ステップＷ９）。

【００６７】上記ステップＷ８においてパケットを結合した後、侵入検出部１１は、すべてのパケットの結合が完了したか否かを判別する（ステップＷ１０）。まだ完了していなければ（ステップＷ１０のＮＯ）、侵入検出部１１は、当該処理を終了する。一方、完了すれば（ステップＷ１０のＹＥＳ）、当該アクセスは正常アクセスである可能性が極めて高いため、侵入検出部１１は、当該構造体を破棄する（ステップＷ１１）。

【００６８】以上のように本実施の形態３によれば、一連のパケットを取得している最中においてパケット結合処理を実行し、正常に組み立てることができない場合に、その時点において構造体の保留を決定する。したがって、構造体の保留／破棄を迅速に決定することができる。そのため、構造体の総数を検査する周期を短くしても、単なるアクセス量の増大を不正アクセスであると誤検出することがない。よって、不正アクセス検出に要する時間を短縮することができ、被害拡大を迅速に防ぐことができる。

【００６９】実施の形態４

図１２は、本発明の実施の形態４に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。図１２において、図１と同じ機能部分については同一の参照符号を使用する。

【００７０】上記実施の形態１ないし３では、１つの内部ネットワーク３が１つのルータ２を介して外部ネットワーク１に接続されている構成を例にとっている。これに対して、本実施の形態４では、複数の内部ネットワーク２０Ａ、２０Ｂを有し、当該複数の内部ネットワーク２０Ａ、２０Ｂと外部ネットワーク１とをそれぞれルータ２１Ａ、２１Ｂを介して接続した構成を例にとってい

る。

【００７１】より具体的には、このコンピュータシステムは、２つの内部ネットワーク２０Ａ、２０Ｂを有し、いずれもルータ２１Ａ、２１Ｂを介して外部ネットワーク１に接続されている。各内部ネットワーク２０Ａ、２０Ｂ同士もまた、ルータ２２を介して接続されている。２つの内部ネットワーク２０Ａ、２０Ｂは、たとえば同じ企業の異なる部署内に構築されている。すなわち、本実施の形態４では、不正アクセスを同時期に受ける可能性のある２つの内部ネットワーク２０Ａ、２０Ｂを有するコンピュータネットワークを前提にしている。さらに、このコンピュータネットワークは、上位管理装置２３を備えている。上位管理装置２３は、内部ネットワークに関連して設けられ、２つのルータ２１Ａ、２１Ｂに専用線２４Ａ、２４Ｂを介して接続されている。

【００７２】図１３は、上記２つのルータ２１Ａ、２１Ｂおよび上位管理装置２３の内部構成を示すブロック図である。２つのルータ２１Ａ、２１Ｂは、いずれも、実施の形態１ないし３と同様に、ルーチング部１０および侵入検出部１１を有している。このうち侵入検出部１１は、実施の形態１ないし３のいずれかと同様に、セションごとに構造体を生成して一定期間ごとにその数を検証することにより不正アクセスの検出を行っている。また、各ルータ２１Ａ、２１Ｂは、不正アクセスの侵入を検出した場合に、不正アクセス検出信号を専用線２４Ａ、２４Ｂを介して上位管理装置２３に送信する。不正アクセス検出信号は、不正アクセスを検出したことを示すデータを含むものである。

【００７３】上位管理装置２３は、侵害判定部２３ａを有している。侵害判定部２３ａは、２つのルータ２１Ａ、２１Ｂから不正アクセス検出信号を受信したか否かに基づいて、不正アクセスの侵入の有無を判定するものである。上述のように、２つのルータ２１Ａ、２１Ｂは、不正アクセスを同時期に受ける可能性のあるものである。したがって、一方のルータで不正アクセスが検出された場合、他方のルータでも不正アクセスが検出される可能性がある。しかし、一方のルータにおいて不正アクセスであると検出された場合であっても、他方のルータにおいてあまり構造体数が多くなければ、単なるアクセス量増加の可能性もある。そのため、上位管理装置２３において、両方のルータ２１Ａ、２１Ｂから不正アクセス検出信号を受信したことを条件として、不正アクセスの侵入があると判定することとしている。判定結果は、不正アクセス検出信号の送信元のルータ、または両方のルータに送信される。

【００７４】図１４は、侵入検出部１１において実行される構造体数検査処理を説明するためのフローチャートである。上述のように、侵入検出部１１は、検出周期の開始に応答して（ステップＸ１のＹＥＳ）、保持している構造体の総数ｎが不正検出しきい値ｎｔｈ以上であるか否かを判別する（ステップＸ２）。構造体の総数ｎが不正検出しきい値ｎｔｈ未満であれば（ステップＸ２のＮＯ）、侵入検出部１１は、当該処理を終了する。一方、構造体の総数ｎが不正検出しきい値ｎｔｈ以上であれば（ステップＸ２のＹＥＳ）、侵入検出部１１は、ポート遮断をルーチング部１０に通知するのに先立って、不正アクセス検出信号を作成し、当該不正アクセス検出信号を専用線２４Ａまたは２４Ｂを介して上位管理装置２３に送信する（ステップＸ３）。

【００７５】上位管理装置２３は、後述するように、他方のルータから不正アクセス検出信号を受信したか否かに応じて判定信号をルータに送信する。そこで、侵入検出部１１は、不正アクセス検出信号を上位管理装置２３に送信した後、判定信号を受信したか否かを判別する（ステップＸ４）。

【００７６】判定信号を受信した場合、当該判定信号が肯定を示していれば、確かに不正アクセスが発生していると考えられるから、侵入検出部１１は、ルーチング部１０にアクセスし、外部ネットワーク１との接続ポートを遮断させる（ステップＸ５）。一方、判定信号を受信した場合に当該判定信号が否定を示していれば、単なるアクセス量の増加であると考えられるから、侵入検出部１１は、当該処理を終了する。

【００７７】図１５は、上位管理装置２３の侵害判定部２３ａにおける侵害判定処理を説明するためのフローチャートである。侵害判定部２３ａは、不正アクセス検出信号を受信したか否かを判別する（ステップＹ１）。不正アクセス検出信号を受信すると（ステップＹ１のＹＥＳ）、侵害判定部２３ａは、他方のルータから不正アクセス検出信号を受信したか否かを判別する（ステップＹ２）。侵害判定部２３ａは、当該判別処理の開始から予め定められた一定時間が経過したか否かを判別し（ステップＹ３）、上記一定時間が経過するまで上記判別処理を繰り返し実行する。２つのルータから不正アクセス検出信号が送信されるのにはある程度の時間差があることが予想され、上記一定時間は上記時間差を考慮して設定されている。

【００７８】上記ステップＹ３において一定時間が経過したと判別されるまでの間に、上記ステップＹ２において他方のルータから不正アクセス検出信号を受信したと判別されると、侵害判定部２３ａは、不正アクセスの発生を肯定する判定信号を両方のルータに送信する（ステップＹ４）。一方、上記ステップＹ２において他方のルータから不正アクセス検出信号を受信したと判別されないまま上記一定時間が経過した場合、不正アクセス検出信号の送信元であるルータへの単なるアクセス量の増加であると考えられるから、侵害判定部２３ａは、不正アクセスの発生を否定する判定信号を上記送信元のルータに送信する（ステップＹ５）。

【００７９】図１６は、上述のルータ２１Ａ、２１Ｂの

構成を機能的に説明するための概念図である。ルータ２１Ａ、２１Ｂは、いずれも、通信プロトコルの階層として、物理層、データリンク（Ｄ／Ｌ）層、ＩＰ層、ＴＣＰ層および上位ＡＰ層を有している。ルータ２１は、パケットをネットワーク層であるＩＰ層あるいはトランスポート層であるＴＣＰ層で管理している。ＩＰ層またはＴＣＰ層での管理結果は、上位管理装置２３に通知される。

【００８０】以上のようにこの実施の形態４によれば、複数のルータにて不正アクセスの侵入が検出された場合に、それらの検出結果を一元的に集めることにより、不正アクセスの侵入があるか否かを判定している。したがって、１つのルータにおいて不正アクセスを検出するよりも、不正アクセスを受けていることを高精度に判断することができる。そのため、セキュリティの信頼性をより一層高めることができる。

【００８１】なお、上述の説明では、２つの内部ネットワーク２０Ａ、２０Ｂがそれぞれルータ２１Ａ、２１Ｂを介して外部ネットワーク１に接続されている構成を例にとっている。しかし、３以上の内部ネットワーク３をそれぞれルータを介して外部ネットワーク１に接続しているコンピュータネットワークにおいても、当該実施の形態４と同様の構成を採用することができる。

【００８２】実施の形態５

上記実施の形態４では、上位管理装置２３において複数のルータ２１Ａ、２１Ｂへのアクセス状況を監視し、上位管理装置２３において不正アクセス検出の最終判断を行っており、ルータ２１Ａ、２１Ｂは単に上位管理装置２３の判断に従うのみである。これに対して、本実施の形態５では、１つのルータにおいて不正アクセスの侵入が検出された場合、当該ルータが他のルータのアクセス状況を参照することにより、不正アクセスであるか否かの最終判断をルータ自身において行うこととしている。

【００８３】より詳述すれば、本実施の形態５に係るコンピュータシステムは、上記実施の形態４と同様に、２つの内部ネットワーク２０Ａ、２０Ｂをそれぞれルータ２１Ａ、２１Ｂを介して外部ネットワーク１に接続した構成となっており、内部ネットワーク２０Ａ、２０Ｂに関連して各ルータ２１Ａ、２１Ｂに接続された上位管理装置２３を備えている。当該コンピュータシステムは、さらに、図１２に破線で示すように、ルータ２１Ａ、２１Ｂ同士を専用線３０を介して相互接続している。より具体的には、当該コンピュータシステムは、図１３に破線で示すように、各ルータ２１Ａ、２１Ｂ内の侵入検出部１１同士を専用線３０を介して相互接続している。

【００８４】図１７は、本実施の形態５に係る構造体数検査処理を説明するためのフローチャートである。侵入検出部１１は、上述のように、侵入検出部１１は、検出周期の開始に応答して（ステップＺ１のＹＥＳ）、保持している構造体の総数ｎが不正検出しきい値ｎth以上であるか否かを判別する（ステップＺ２）。構造体の総数ｎが不正検出しきい値ｎth未満であれば（ステップＺ２のＮＯ）、侵入検出部１１は、当該処理を終了する。一方、構造体の総数ｎが不正検出しきい値ｎth以上であれば（ステップＺ２のＹＥＳ）、侵入検出部１１は、ポート遮断をルーチング部１０に通知するのに先立って、アクセス状況確認信号を作成し、当該アクセス状況確認信号を専用線を介して他のルータに送信する（ステップＺ３）。上記アクセス状況確認信号は、他のルータのアクセス状況を確認するためのものである。より具体的には、上記アクセス状況確認信号は、他のルータのアクセス状況の返信を指示するメッセージを含むものである。

【００８５】他のルータは、後述するように、自ルータのアクセス状況、具体的には構造体の総数ｎを含む返信信号を送信元のルータに返信する。そこで、侵入検出部１１は、返信信号を受信したか否かを判別する（ステップＺ４）。返信信号を受信した場合（ステップＺ４のＹＥＳ）、侵入検出部１１は、当該返信信号に含まれている構造体の総数ｎに基づいて、他のルータのアクセス状況を確認する（ステップＺ５）。

【００８６】より具体的には、侵入検出部１１は、上記返信信号に含まれている構造体の総数ｎが上記不正検出しきい値ｎthよりも小さな第２のしきい値ｋth以上であるか否かを判別する。上記第２のしきい値ｋthは、これ以上構造体があれば不正アクセスである蓋然性が高いと考えられる値に設定されている。たとえば、第２のしきい値ｋthは、不正検出しきい値ｎthよりも数１０％ほど小さな値である。

【００８７】上記構造体の総数ｎが第２のしきい値ｋth未満であれば、自ルータに対してのみアクセス量が増加していると考えられるから、侵入検出部２２は、当該処理を終了する。一方、上記構造体の総数ｎが第２のしきい値ｋth以上であれば、他のルータにおいてもアクセス量が非常に多く不正アクセスである蓋然性が非常に高いと考えられるから、侵入検出部１１は、ルーチング部１０にアクセスして外部ネットワーク１との接続ポートの遮断を指示する（ステップＺ６）。また、侵入検出部１１は、不正アクセスの侵入を検出した旨のメッセージを含む報告信号を上位管理装置２３に送信する（ステップＺ７）。

【００８８】図１８は、本実施の形態５に係る侵入検出部１１におけるアクセス状況返信処理を説明するためのフローチャートである。このアクセス状況返信処理は、上記構造体数検査処理と並列に行われるものである。

【００８９】侵入検出部１１は、他のルータからアクセス状況確認信号を受信したか否かを判別する（ステップＲ１）。アクセス状況確認信号を受信した場合、侵入検出部１１は、アクセス状況を送信元のルータに通知する（ステップＲ２）。より具体的には、アクセス状況を含む返信信号を送信元のルータに送信する。さらに具体的

には、構造体記憶部１１ｂに記憶されている構造体の総数ｎを含む返信信号を作成し、当該返信信号を送信元のルータに送信する。

【００９０】図１９は、上述のルータ２１Ａ、２１Ｂの構成を機能的に説明するための概念図である。ルータ２１Ａ、２１Ｂは、いずれも、通信プロトコルの階層として、物理層、データリンク（Ｄ／Ｌ）層、ＩＰ層、ＴＣＰ層および上位ＡＰ層を有している。ルータ２１のＴＣＰ層は、不正アクセスの侵入の有無を検出する。ルータ２１のＴＣＰ層は、その検出結果を他方のルータ２１のＴＣＰ層に通知し、他方のルータ２１のＴＣＰ層からアクセス状況の通知を受ける。また、ルータ２１のＴＣＰ層は、当該アクセス状況を上位管理装置に通知する。

【００９１】以上のように本実施の形態５によれば、他のルータのアクセス状況を確認することにより、ルータ内の侵入検出部自身において不正アクセスの侵入の有無を判別している。したがって、上位管理装置２３にて両方の不正アクセス検出信号を待って不正アクセスであるか否かを判定するよりも、不正アクセスであることを迅速に判断することができる。そのため、不正アクセスに対する措置を迅速にとることができる。

【００９２】なお、上述の説明では、２つの内部ネットワーク２０Ａ、２０Ｂがそれぞれルータ２１Ａ、２１Ｂを介して外部ネットワーク１に接続されている構成を例にとっている。しかし、３以上の内部ネットワーク３をそれぞれルータを介して外部ネットワーク１に接続しているコンピュータネットワークにおいても、当該実施の形態５と同様の構成を採用することができる。

【００９３】実施の形態６

図２０は、本発明の実施の形態６に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。図２０において、図１と同じ機能部分については同一の参照符号を使用する。

【００９４】上記実施の形態５では、自ルータのアクセス量の増加が不正アクセスであるか否かを確認するために、他のルータのアクセス状況を参照している。これに対して、本実施の形態６では、自ルータのアクセス量の増加が不正アクセスであるか否かを確認するために他のルータのアクセス状況を参照するとともに、他のルータの不正検出しきい値ｎｔｈを他のルータ自身で補正することとしている。

【００９５】より詳述すれば、複数のルータは、上述のように、各々同一の不正検出しきい値ｎｔｈを使用して不正アクセス検出を行っている。一方、複数のルータは不正アクセスを同時に受ける可能性のあるもの同士であるので、１つのルータにおいて不正アクセスが検出されれば、他のルータにおいても不正アクセスを受けている可能性がある。しかし、構造体の数が不正検出しきい値ｎｔｈ以上となるタイミングはルータによってばらつく場合が多く、しかもそのタイミングのばらつきは以後の不正アクセスにおいても同様の傾向を示すものと考えられる。そこで、本実施の形態７では、不正アクセス検出のタイミングのずれを考慮し、不正検出しきい値ｎｔｈをルータ単位で動的に補正することにより、不正アクセスの検出速度を向上させ、被害拡大を迅速に阻止し得るようにしている。

【００９６】本実施の形態６に係るコンピュータネットワークは、複数の内部ネットワーク４０Ａ、４０Ｂ、４０Ｃ、４０Ｄを有し、各々ルータ４１Ａ、４１Ｂ、４１Ｃ、４１Ｄ（以下総称するときは「ルータ４１」という）を介して外部ネットワーク１に接続されている。これら各ルータ４１Ａ、４１Ｂ、４１Ｃ、４１Ｄは、論理的に隣接するルータと専用線４２を介して接続されている。より具体的には、複数のルータ４１Ａ～４１Ｄは、専用線４２を介して環状に接続されている。また、このコンピュータネットワークは、複数の内部ネットワーク４０Ａ～４０Ｄに関連して設けられた上位管理装置４３を備えている。上位管理装置４３は、各ルータ４１Ａ、４１Ｂ、４１Ｃ、４１Ｄに専用線４４Ａ、４４Ｂ、４４Ｃ、４４Ｄを介してそれぞれ接続され、すべてのルータ４１Ａ～４１Ｄにおけるアクセス状況を監視する機能を有している。なお、内部ネットワーク４０同士もルータ４６を介してそれぞれ相互接続されている。

【００９７】図２１は、複数のルータ４１の内部構成を示すブロック図である。各ルータ４１は、上記実施の形態１ないし５と同様に、それぞれ、侵入検出部１１およびルーチング部１０を備えている。各侵入検出部１１は、論理的に隣接するルータ４１の侵入検出部１１と専用線４２を介して相互接続されている。また、各侵入検出部１１は、複数の補正しきい値ｍｔｈを記憶する補正しきい値記憶部５０を有している。上記補正しきい値ｍｔｈは、少なくとも不正検出しきい値ｎｔｈよりも小さな値で、アクセス量が急激に増加したときに不正検出しきい値ｎｔｈの補正値として利用されるものである。補正しきい値ｍｔｈは、たとえば、不正検出しきい値ｎｔｈよりも数％ずつ小さくなる複数の値である。なお、補正しきい値ｍｔｈを１つだけ設定してもよいことはもちろんである。

【００９８】図２２は、侵入検出部１１における構造体数検査処理を説明するためのフローチャートである。侵入検出部１１は、検出周期の開始に応答して（ステップＮ１のＹＥＳ）、構造体記憶部１１ｂに保有している構造体の総数ｎがしきい値記憶部１１ａに記憶されている不正検出しきい値ｎｔｈ以上であるか否かを判別する（ステップＮ２）。構造体の総数ｎが不正検出しきい値ｎｔｈ未満であれば（ステップＮ２のＮＯ）、侵入検出部１１は、当該処理を終了する。一方、構造体の総数ｎが不正検出しきい値ｎｔｈ以上であれば（ステップＮ２のＹＥＳ）、侵入検出部１１は、ポート遮断をルーチング部１０に通知するのに先立って、補正指示信号を作成し、当該補正指示信号を専用線４２を介して隣接するルータ４

１に送信する（ステップＮ３）。上記補正指示信号は、上記構造体の総数ｎと不正検出しきい値ｎｔｈの補正を指示する旨のメッセージとを含むものである。

【００９９】１つのルータの侵入検出部から補正指示信号が送信されると、他のすべてのルータの侵入検出部は、各々のアクセス状況、具体的には構造体の総数ｎおよび補正の有無結果を含む返信信号を送信元のルータに返信する。そこで、侵入検出部１１は、補正指示信号を送信した後、他のすべての関連するルータから返信信号を受信したか否かを判別する（ステップＮ４）。

【０１００】すべての返信信号を受信すると（ステップＮ４のＹＥＳ）、侵入検出部１１は、当該返信信号に含まれているアクセス状況に基づいて、自ルータのアクセス量増加は不正アクセスであるか否かを判別する（ステップＮ５）。より具体的には、侵入検出部１１は、構造体の総数ｎが第２のしきい値ｋｔｈ以上であるか否かをすべての返信信号について判別する。また、侵入検出部１１は、当該判別結果に基づいて、構造体の総数ｎが第２のしきい値ｋｔｈ以上である割合が一定割合以上であるか否かを判別する。

【０１０１】一定割合以上であれば、他のルータでもアクセス量が急激に増加して不正アクセスである蓋然性が高いと考えられるから、侵入検出部１１は、ルーチング部１０に対して接続ポートを遮断させる（ステップＮ６）。その後、ステップＮ７に移行する。一方、一定割合未満であれば、単なるアクセス量の増加と考えられるから、侵入検出部１１は、ステップＮ７に直接移行する。

【０１０２】ステップＮ７は、関連するすべてのルータ４１における補正状況を上位管理装置に通知する処理である。より具体的には、侵入検出部１１は、返信信号に含まれている補正の有無結果を上位管理装置４３に送信する。これにより、上位管理装置４３は、関連するすべてのルータ４１の不正検出しきい値ｎｔｈの状況を一元管理することができる。

【０１０３】図２３は、侵入検出部１１のアクセス状況返信処理を説明するためのフローチャートである。侵入検出部１１は、補正指示信号を受信すると（ステップＭ１）、不正検出しきい値ｎｔｈの補正の必要性を判断する（ステップＭ２）。より具体的には、侵入検出部１１は、構造体記憶部１１ｂに記憶されている構造体の総数ｎと補正しきい値記憶部５０に記憶されている補正しきい値ｍｔｈとを比較し、構造体の総数ｎがすべての補正しきい値ｍｔｈ以上であるか否かを判別する。

【０１０４】構造体の総数ｎよりも大きな補正しきい値ｍｔｈがある場合（ステップＭ２のＮＯ）、補正の必要があるから、侵入検出部１１は、現在の不正検出しきい値ｎｔｈを補正する（ステップＭ３）。より具体的には、侵入検出部１１は、複数の補正しきい値ｍｔｈのうち現在の不正検出しきい値ｎｔｈよりも小さく、かつその中で最も大きな補正しきい値ｍｔｈを特定する。侵入検出部１１は、この特定された補正しきい値ｍｔｈを新たな不正検出しきい値ｎｔｈとして設定する。その後、侵入検出部１１は、アクセス状況、具体的には上記構造体の総数ｎと補正有のメッセージとを含む返信信号を作成し、当該返信信号を送信元のルータ４１に返信する（ステップＭ４）。

【０１０５】一方、構造体の総数ｎがすべての補正しきい値ｍｔｈ以上である場合（ステップＭ２のＹＥＳ）、補正の必要はないから、侵入検出部１１は、不正検出しきい値ｎｔｈを補正することなく、アクセス状況、具体的には構造体の総数ｎと補正無のメッセージとを含む返信信号を作成し、当該返信信号を送信元のルータ４１に返信する（ステップＭ５）。

【０１０６】さらに、侵入検出部１１は、上記受信された補正指示信号を論理的に隣接する２つのルータのうち、補正指示信号を送信してきたルータとは別のルータに対して、上記補正指示信号を転送する（ステップＭ６）。

【０１０７】図２４は、上述の４つのルータのうちルータ４１Ａ、４１Ｂ、４１Ｃの構成を機能的に説明するための概念図である。ルータ４１は、通信プロトコルの階層として、物理層、データリンク（Ｄ／Ｌ）層、ＩＰ層、ＴＣＰ層および上位ＡＰ層を有している。

【０１０８】たとえばルータ４１ＡのＴＣＰ層において不正アクセスが検出された場合、当該ルータ４１Ａの上位ＡＰ層は、不正アクセスを検出したことおよび構造体の総数ｎを隣接するルータ４１Ｂの上位ＡＰ層に通知する。ルータ４１Ｂの上位ＡＰ層は、当該通知に応答して不正検出しきい値ｎｔｈを補正しあるいは補正することなく、アクセス状況および補正の有無を送信元のルータ４１Ａの上位ＡＰ層に返信する。また、ルータ４１Ｂの上位ＡＰ層は、ルータ４１Ａからの通知を隣接するルータ４１Ｃの上位ＡＰ層に通知する。ルータ４１Ｃの上位ＡＰ層は、上記通知に応答して不正検出しきい値ｎｔｈを補正しあるいは補正することなく、アクセス状況および補正の有無をルータ４１Ｂの上位ＡＰ層に返信する。ルータ４１Ｂの上位ＡＰ層は、当該返信内容をさらにルータ４１Ａに返信する。さらに、ルータ４１Ａの上位ＡＰ層は、これら関連するすべてのルータのアクセス状況および／または補正の有無を上位管理装置４３に通知する。

【０１０９】以上のように本実施の形態６によれば、他のルータのアクセス状況を参照することにより、アクセス量の増加が不正アクセスであるか否かを判別している。したがって、不正アクセスの検出精度を向上できる。しかも、他のルータにおいて不正検出しきい値ｎｔｈをアクセス状況に応じて補正しているから、もしもその後不正アクセスがあった場合でもそれを迅速に検出することができる。そのため、被害拡大を最小限に抑えることができる。

【０１１０】実施の形態７
図２５は、本発明の実施の形態７に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。図２５において、図１と同じ機能部分については同一の参照符号を使用する。
【０１１１】上記実施の形態１ないし６では、ルータは到達するすべてのパケットを不正アクセス検出の対象としている。これに対して、本実施の形態７では、１つの内部ネットワークに対して複数のルータを接続し、各ルータを１つのサービス種別にそれぞれ対応付けるとともに、各ルータにおいて対応するサービス種別のパケットのみを不正アクセス検出の対象としている。ただし、対応するサービス種別以外のパケットを無条件に内部ネットワークに進入させるのでなく、そのようなパケットについては別のサーバ（おとりサーバ）に転送し、当該おとりサーバにおいて不正パケットであるか否かを監視することとしている。
【０１１２】複数のサービスを提供する１つの内部ネットワークがある場合、１つのルータですべてのサービス種別のパケットを不正アクセス検出の対象とすると、当該ルータの負荷が大きく、不正パケットであってもそれを看過するおそれがある。そこで、ルータの負荷を軽減すべく、上記内部ネットワークに対して複数のルータを接続するとともに、１つのルータにおいては１つのサービス種別のパケットのみを不正アクセスの検出対象とすることとしている。ただし、上述したように、１つのルータに到達した他のサービス種別のパケットを無条件に通過させるのは危険であるため、各ルータにそれぞれ対応するおとりサーバを設け、当該おとりサーバにて不正アクセスの検出を行うこととしている。
【０１１３】より詳述すれば、１つの内部ネットワーク３は、複数のルータ６０Ａ、６０Ｂ、６０Ｃ（以下総称するときは「ルータ６０」という）を介して外部ネットワーク１に接続されている。各ルータ６０Ａ、６０Ｂ、６０Ｃは、それぞれ、１つのサービス種別に対応している。本実施の形態７に係る内部ネットワーク１が提供するサービス種別は、たとえば、メールサービス、ウェブサービスおよびＦＴＰサービスである。これらのサービス種別は、パケットのヘッダに記述されている送信先ポートにより識別可能である。
【０１１４】各ルータ６０Ａ、６０Ｂ、６０Ｃには、それぞれ、おとりサーバ６１Ａ、６１Ｂ、６１Ｃ（以下総称するときは「おとりサーバ６１」という）が接続されている。各おとりサーバ６１Ａ、６１Ｂ、６１Ｃは、それぞれ、内部ネットワーク３にて提供される複数のサービス種別のうち、接続されているルータ６０Ａ、６０Ｂ、６０Ｃに対応付けられているサービス種別以外のサービス種別のパケットを対象とし、不正アクセスの侵入の有無を検出する。おとりサーバ６１には、ルータ６０にてコピーされたパケットが与えられるようになっている。
【０１１５】図２６は、本実施の形態７に係る侵入検出部１１における構造体生成／破棄処理を説明するためのフローチャートである。なお、本実施の形態７においては、当該構造体生成／破棄処理と並列に、たとえば図７に示された構造体数検査処理が行われる。
【０１１６】侵入検出部１１は、通信路１２からパケットを取得すると（ステップＱ１）、当該パケットのヘッダを抽出する（ステップＱ２）。その後、侵入検出部は、当該抽出されたヘッダ中の送信ポートを参照し、対象パケットであるか否かを判別する（ステップＱ３）。すなわち、対象とするサービス種別に対応するパケットであるか否かを判別する。
【０１１７】対象パケットであれば（ステップＱ３のＹＥＳ）、侵入検出部１１は、上記実施の形態１ないし３のいずれかで説明した構造体の生成／更新および破棄に関する処理を実行する（ステップＱ４）。具体的には、侵入検出部１１は、実施の形態１で説明した図５におけるステップＳ３～Ｓ９の処理を実行する。または、侵入検出部１１は、実施の形態２で説明した図９におけるステップＶ３～Ｖ１３の処理を実行する。または、侵入検出部１１は、実施の形態３で説明した図１１におけるステップＷ３～Ｗ１１の処理を実行する。
【０１１８】一方、対象パケットでなければ（ステップＱ３のＮＯ）、侵入検出部１１は、当該パケットの検査を禁止する（ステップＱ５）。すなわち、当該パケットについて構造体の生成／更新処理を行わない。しかし、何らの検査もしなければ不正アクセスを看過するかもしれないから、侵入検出部１１は、当該パケットをコピーし（ステップＱ６）、当該コピーされたパケットを対応するおとりサーバ６１に転送する（ステップＱ７）。
【０１１９】図２７は、本実施の形態７に係るおとりサーバ６１における構造体生成／破棄処理を説明するためのフローチャートである。このおとりサーバ６１においても、当該構造体生成／破棄処理と並列に、たとえば図７に示された構造体数検査処理を実行する。
【０１２０】おとりサーバ６１は、ルータ６０の侵入検出部１１からパケットを受信すると（ステップＰ１のＹＥＳ）、上記実施の形態１ないし３のいずれかで説明したパケットに対応する構造体の生成／更新および破棄に関する処理を実行する（ステップＰ２）。具体的には、侵入検出部１１は、実施の形態１で説明した図５におけるステップＳ３～Ｓ９の処理を実行する。または、侵入検出部１１は、実施の形態２で説明した図９におけるステップＶ３～Ｖ１３の処理を実行する。または、侵入検出部１１は、実施の形態３で説明した図１１におけるステップＷ３～Ｗ１１の処理を実行する。
【０１２１】これにより、対応するルータ６０において対象とするサービス種別以外のパケットの検査を実行することができる。したがって、おとりサーバ６１におい

て攻撃ログを収集することができる。そのため、不正者探知への応用も可能となる。

【０１２２】図２８は、ルータ６０の構成を機能的に説明するための概念図である。ルータ６０は、通信プロトコルの階層として、物理層、データリンク（Ｄ／Ｌ）層、ＩＰ層、ＴＣＰ層および上位ＡＰ層を有している。また、ルータ６０は、ネットワーク層であるＩＰ層およびトランスポート層であるＴＣＰ層の間にＩＤＳ層を有している。

【０１２３】ルータ２に到達するパケットのうち対象とするサービス種別のパケットは、ＩＰ層およびＴＣＰ層を介してＩＤＳ層において処理され、ヘッダからデータまでを関連付けて監視される。すなわち、ネットワーク層よりも上位層でパケットが管理される。また、対象とするサービス種別以外のパケットは、ＩＰ層からおとりサーバ６１に誘導され、当該おとりサーバ６１にて検査される。

【０１２４】以上のようにこの実施の形態７によれば、１つのルータ６０に対して不正アクセス検出の対象パケットを１つのサービス種別に絞り込んでいるので、すべてのサービス種別のパケットを不正アクセス検出の対象とする場合に比べて、ルータの負荷を大幅に軽減できる。したがって、不正アクセスの検出精度を向上できる。そのため、セキュリティ精度の向上を一層図ることができる。

【０１２５】しかも、対象のサービス種別以外のパケットについては、コピーをしておとりサーバ６１に転送し、当該おとりサーバ６１にて不正アクセスの検出対象としている。したがって、サービス種別以外の不正パケットについても検出することができる。そのため、１つのサービス種別につき不正アクセス検出の確実性を向上できるから、全体として、不正アクセス検出の精度を向上できる。よって、セキュリティ精度の向上を図ることができる。

【０１２６】なお、上述の説明では、１つの内部ネットワーク３が複数のサービスを提供する場合を例にとって説明している。しかし、たとえば内部ネットワーク３が１つのサービスのみを提供する場合には、内部ネットワーク３を１つのルータを介して外部ネットワーク１に接続し、当該ルータを上記１つのサービス種別に対応付けるようにすればよい。

【０１２７】他の実施の形態本発明の実施の形態の説明は以上のとおりであるが、本発明は上述の実施の形態以外にも適用可能である。たとえば上記すべての実施の形態においては、EtherIIフレームだけでなく、Ethernet802.3フレーム、Ethernet802.2フレーム、EthernetSNAPなどすべてのEtherフレームを用いることができる。

【０１２８】

【発明の効果】以上のように本発明によれば、パケットのヘッダに記述されているネットワーク層およびトランスポート層のデータに基づいてセションごとに対応する構造体を生成し、当該構造体が異常な数になった場合に不正アクセスの侵入を検出する。したがって、大量の異なるセションを確立するＤＤｏＳ攻撃などの不正アクセスの侵入を精度良く検出できる。また、過去ログを解析することなく不正アクセスの侵入を自動的に検出できる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。

【図２】　パケットの構成を示す概念図である。

【図３】　ルータの内部構成を示すブロック図である。

【図４】　構造体を示す概念図である。

【図５】　構造体生成／破棄処理を説明するためのフローチャートである。

【図６】　構造体破棄処理を説明するためのフローチャートである。

【図７】　構造体数検査処理を説明するためのフローチャートである。

【図８】　本実施の形態２に係る構造体を示す概念図である。

【図９】　本実施の形態２に係る構造体生成／破棄処理である。

【図１０】　ルータの構成を機能的に説明するための概念図である。

【図１１】　本実施の形態３に係る構造体生成／破棄処理を説明するためのフローチャートである。

【図１２】　本発明の実施の形態４に係る侵入検出装置が用いられるコンピュータネットワークの全体構成を示す概念図である。

【図１３】　２つのルータおよび上位管理装置の内部構成を示すブロック図である。

【図１４】　侵入検出部において実行される構造体数検査処理を説明するためのフローチャートである。

【図１５】　上位管理装置の侵害判定部における侵害判定処理を説明するためのフローチャートである。

【図１６】　上述のルータの構成を機能的に説明するための概念図である。

【図１７】　本実施の形態５に係る構造体数検査処理を説明するためのフローチャートである。

【図１８】　本実施の形態５に係る侵入検出部におけるアクセス状況返信処理を説明するためのフローチャートである。

【図１９】　ルータの構成を機能的に説明するための概念図である。

【図２０】　本発明の実施の形態６に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。

【図２１】　複数のルータの内部構成を示すブロック図

である。

【図２２】　侵入検出部における構造体数検査処理を説明するためのフローチャートである。

【図２３】　侵入検出部のアクセス状況返信処理を説明するためのフローチャートである。

【図２４】　上述の４つのルータのうち３つのルータの構成を機能的に説明するための概念図である。

【図２５】　本発明の実施の形態７に係る侵入検出装置が用いられたコンピュータネットワークの全体構成を示す概念図である。

【図２６】　本実施の形態７に係る侵入検出部における構造体生成／破棄処理を説明するためのフローチャートである。

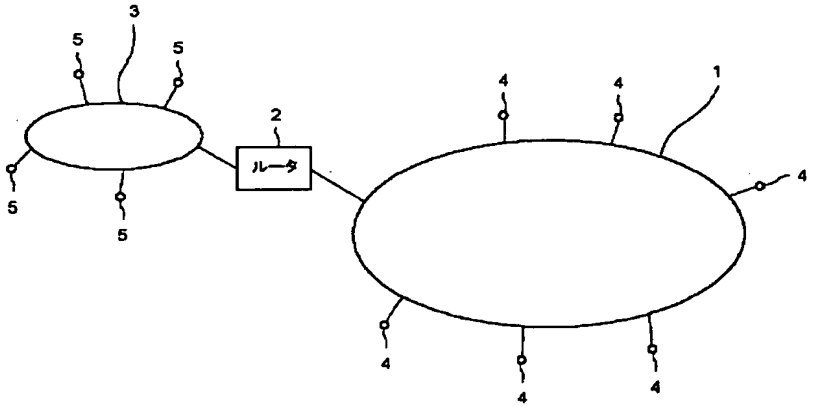
＊【図２７】　本実施の形態７に係るおとりサーバにおける構造体生成／破棄処理を説明するためのフローチャートである。

【図２８】　ルータの構成を機能的に説明するための概念図である。

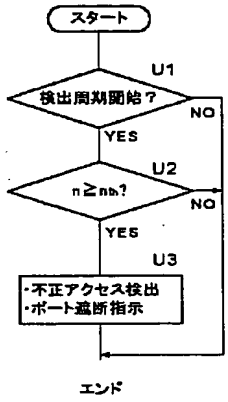
【符号の説明】

１　外部ネットワーク、２　ルータ、３　内部ネットワーク、１１　侵入検出部、１１ａ　しきい値記憶部、１１ｂ　構造体記憶部、２１Ａ、２１Ｂ　ルータ、２３　上位管理装置、２３ａ　侵入判定部　４０Ａ～４０Ｄ　内部ネットワーク、４１Ａ～４１Ｄ　ルータ、４３　上位管理装置、５０　補正しきい値記憶部、６０Ａ～６０Ｃ　ルータ、６１Ａ～６１Ｃ　おとりサーバ。

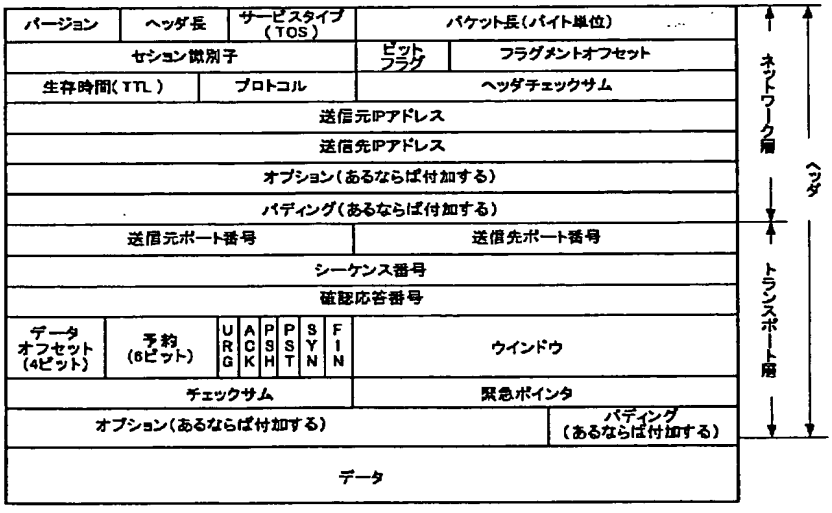
【図１】



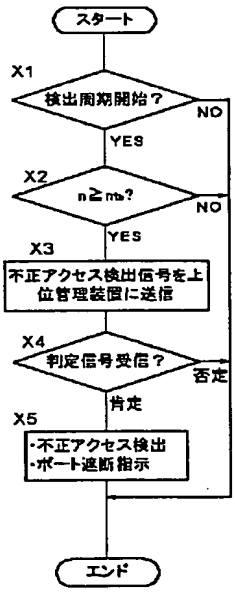
【図７】



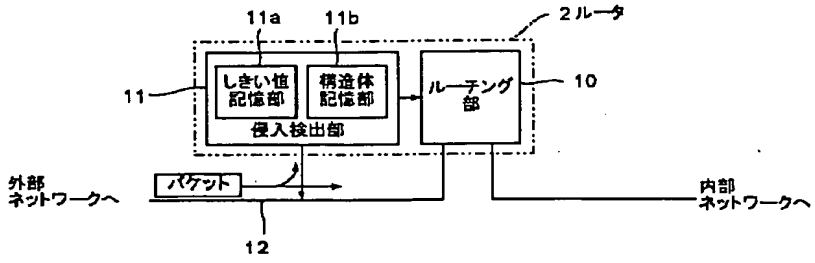
【図２】



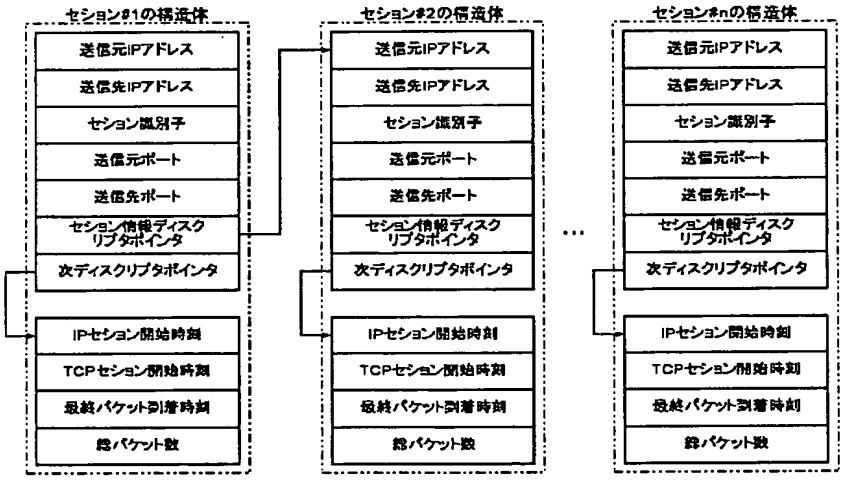
【図１４】



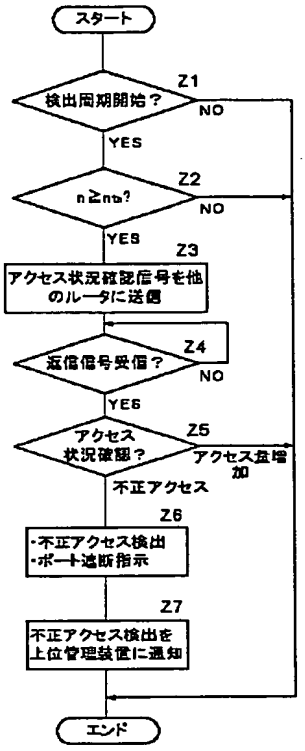
【図３】



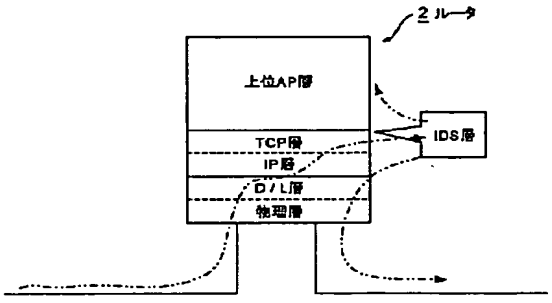
【図４】



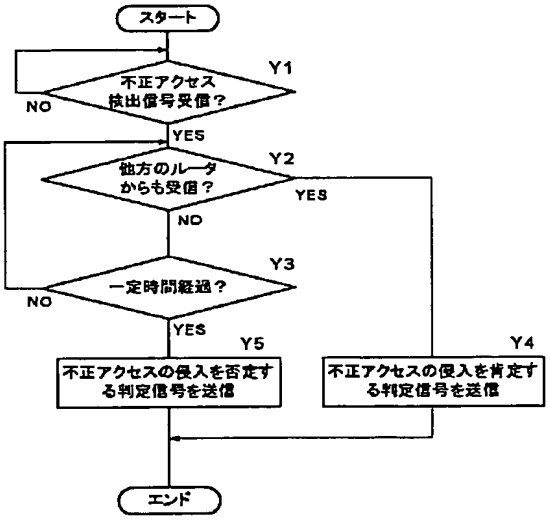
【図１７】



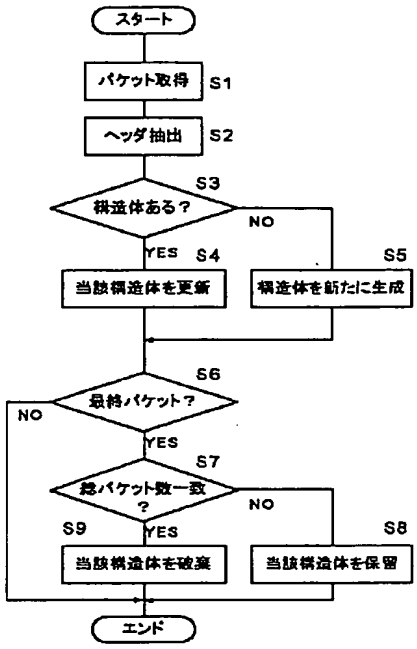
【図１０】



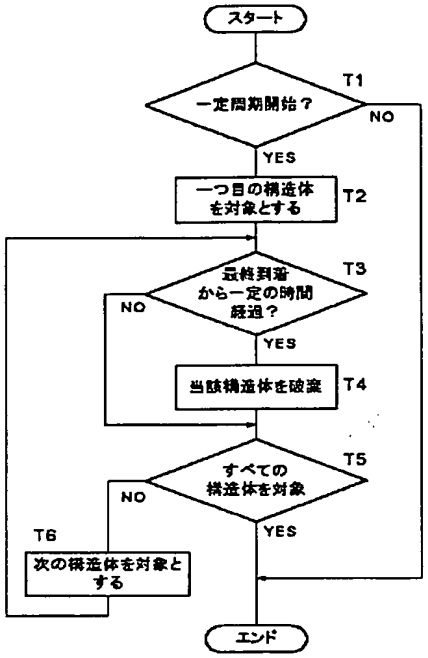
【図１５】



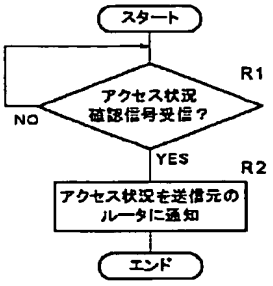
【図５】



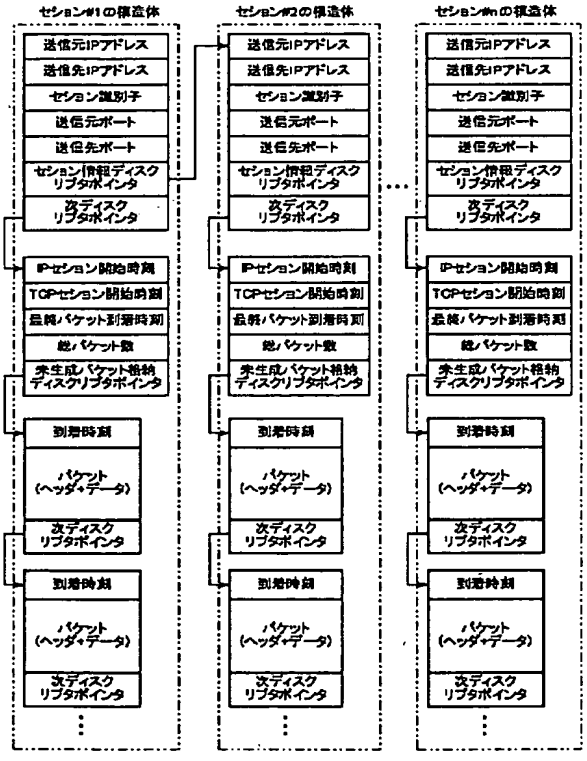
【図６】



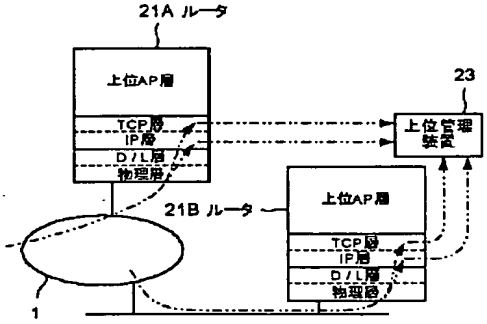
【図１８】



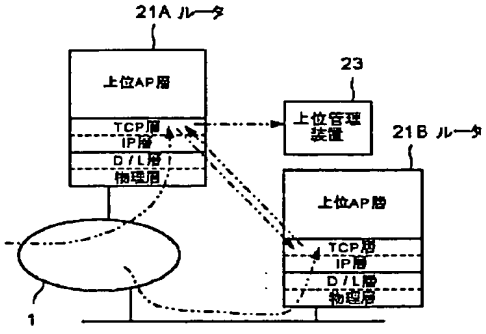
【図８】



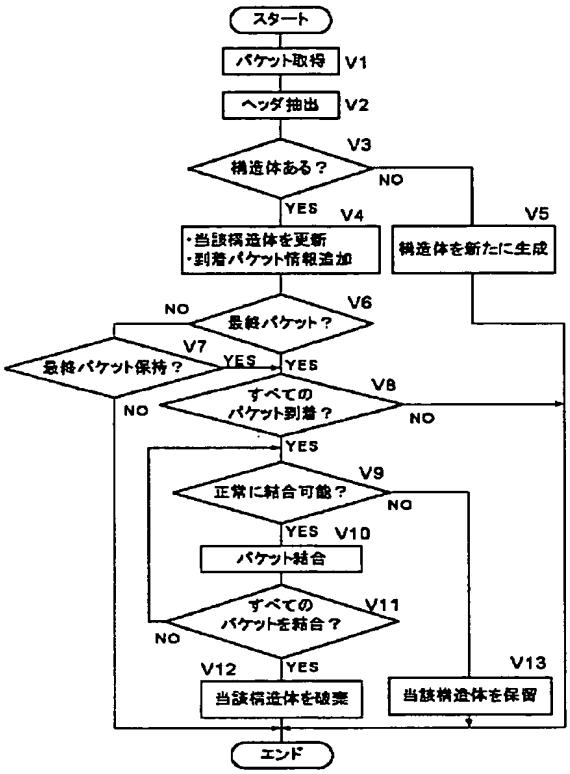
【図１６】



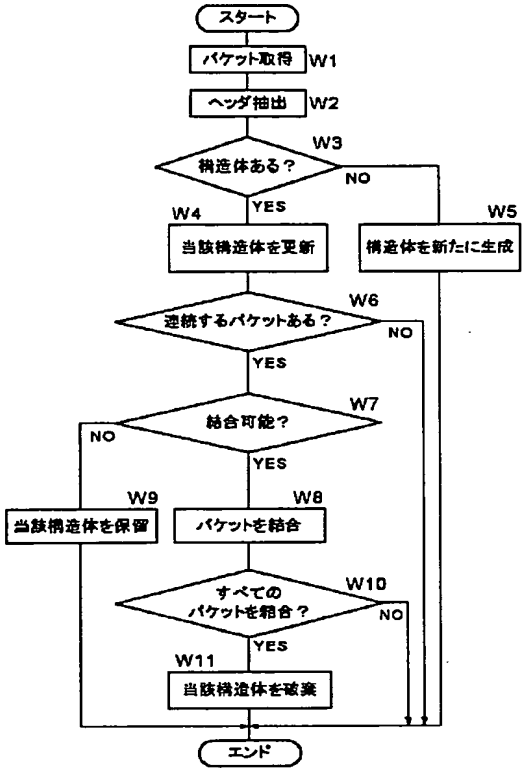
【図１９】



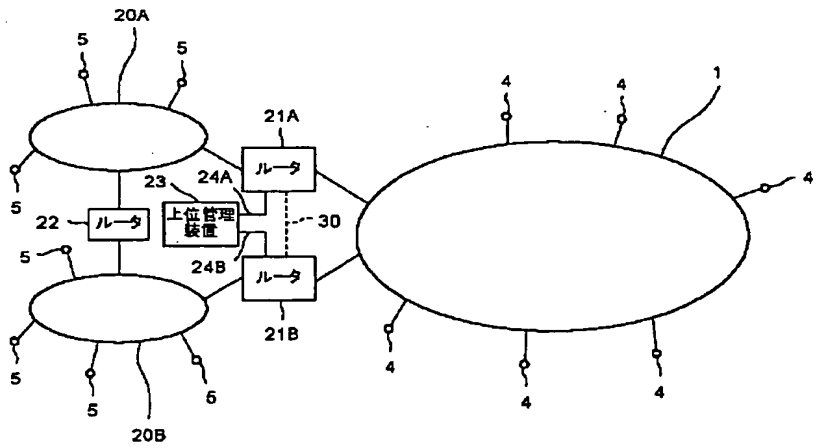
【図９】



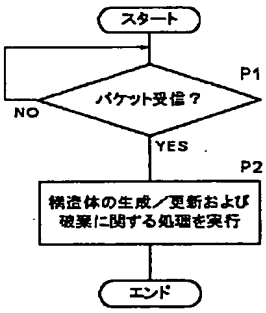
【図１１】



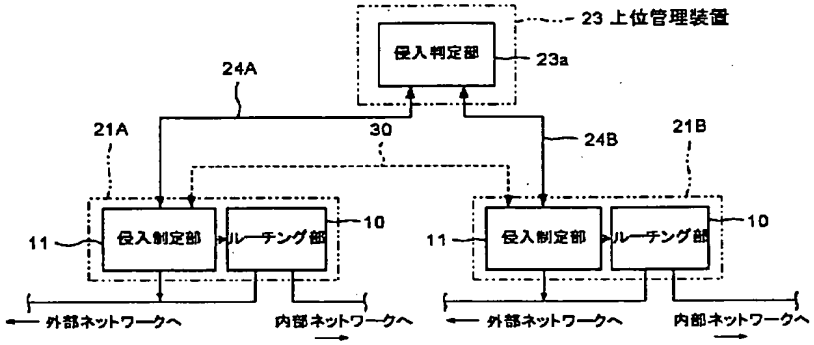
【図１２】



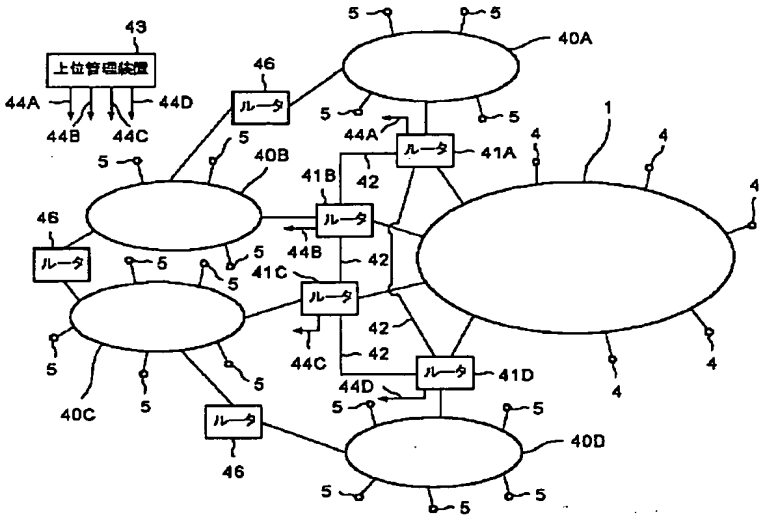
【図２７】



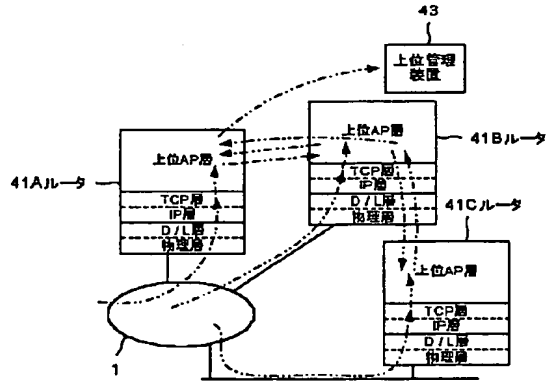
【図１３】



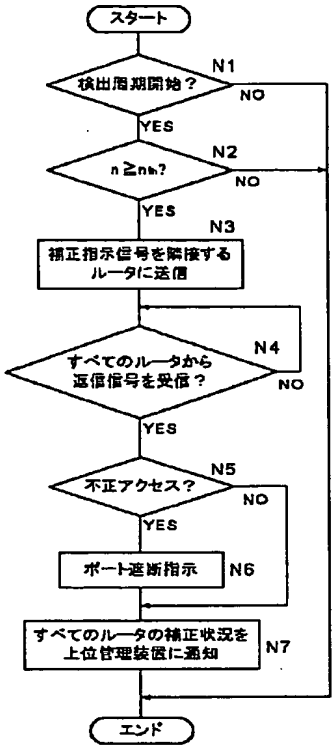
【図２０】



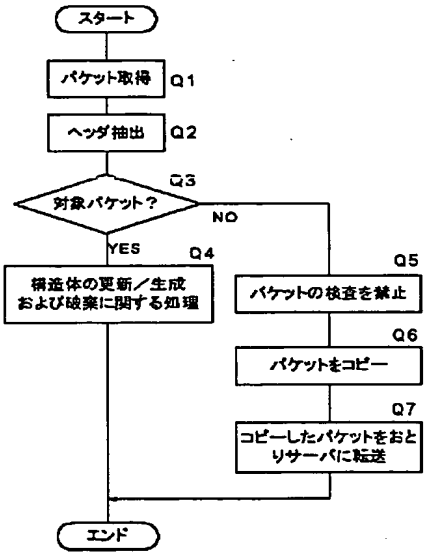
【図２４】



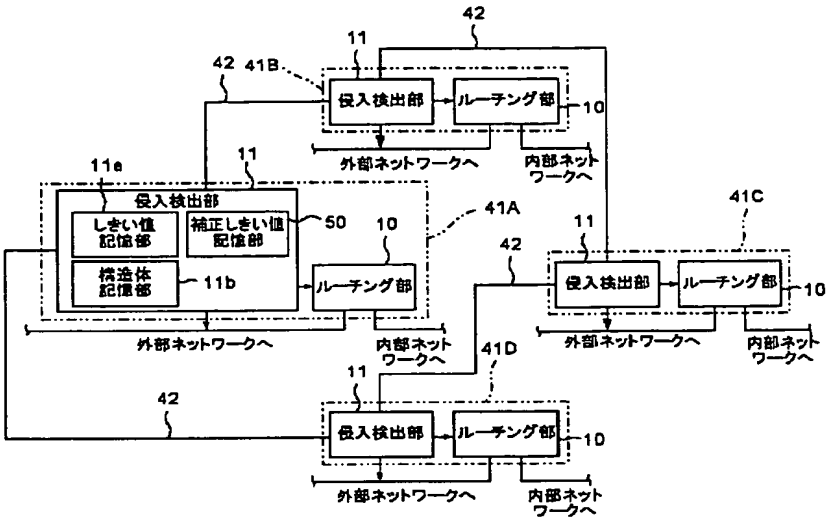
【図２２】



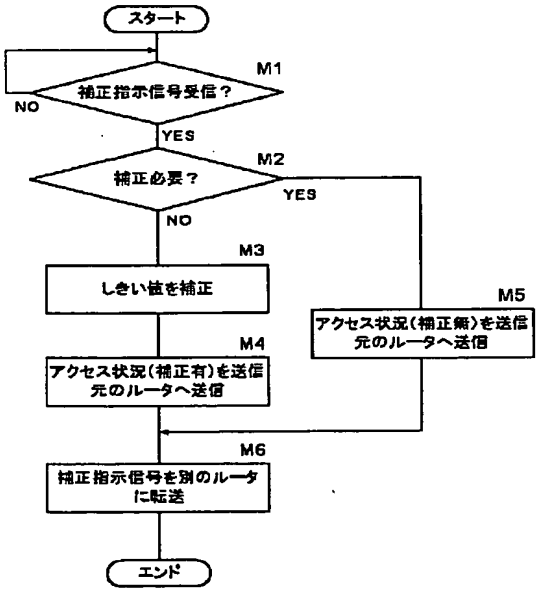
【図２６】



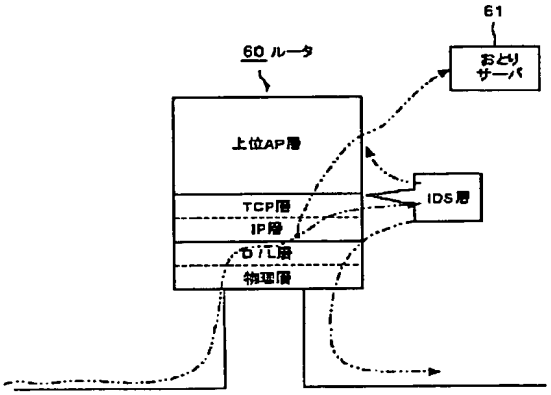
【図２１】


42
11
42
41B
侵入検出部
ルーチング部
10
外部ネットワークへ
内部ネットワークへ
11e
11
侵入検出部
しきい値記憶部
補正しきい値記憶部
50
10
41A
構造体記憶部
11b
ルーチング部
外部ネットワークへ
内部ネットワークへ
41C
11
42
侵入検出部
ルーチング部
10
外部ネットワークへ
内部ネットワークへ
41D
11
42
侵入検出部
ルーチング部
10
外部ネットワークへ
内部ネットワークへ

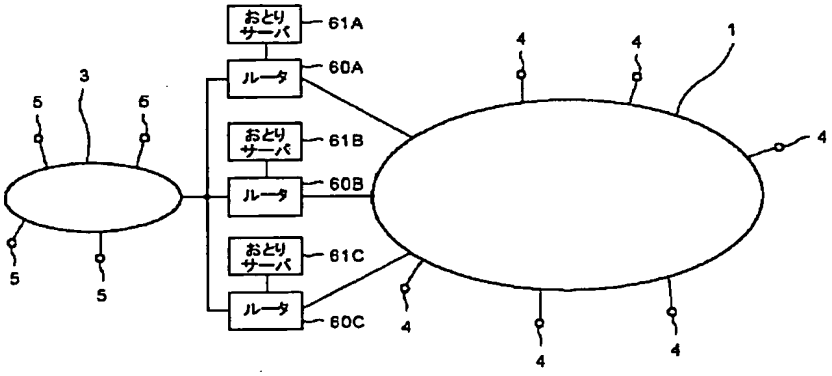
【図２３】


スタート
M1
補正指示信号受信？
NO
YES
M2
補正必要？
YES
NO
M3
しきい値を補正
M5
アクセス状況(補正無)を送信元のルータへ送信
M4
アクセス状況(補正有)を送信元のルータへ送信
M6
補正指示信号を別のルータに転送
エンド

【図２８】


61
60 ルータ
おとりサーバ
上位AP層
TCP層
IP層
MAC層
物理層
IDS層

【図２５】


おとりサーバ
61A
ルータ
60A
おとりサーバ
61B
ルータ
60B
おとりサーバ
61C
ルータ
60C
1
3
4
5
6